SMC® Networks

USER GUIDE

300Mbps Wireless-N Access Point/Repeater

SMCWEBS-N

SMCWEBS-N
User Guide

SMC® Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

January 2010
Pub. # 149100000065W
E012010-AP-R01

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2010 by

SMC Networks, Inc.

20 Mason

Irvine, CA 92618

All rights reserved

Trademarks:

SMC is a registered trademark; and Barricade, EZ Switch, TigerStack, TigerSwitch, and TigerAccess are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Warranty and Product Registration

To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http://www.smc.com.

COMPLIANCES

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

IC STATEMENT

This Class B digital apparatus complies with Canadian ICES-003.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

IMPORTANT NOTE:

IC RADIATION EXPOSURE STATEMENT:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

TAIWAN NCC

根據國家通信傳播委員會低功率電波輻射性電機管理辦法規定：

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

EC CONFORMANCE DECLARATION CE

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1: 2006 (IEC 60950-1) — Product Safety
- EN 55022:2006 + A1:2007, Class B — ITE EMC
- EN 55024:1998 + A1:2001 + A2:2003 — ITE EMC
- EN 300 328 V1.7.1 (2006-10) — Technical requirements for 2.4 GHz radio equipment
- EN 301 489-1 V1.8.1 (2008-04) — EMC requirements for radio equipment
- EN 301 489-17 V1.3.2 (2008-04) — EMC requirements for radio equipment
- 50385 (2002) — Country-specific SAR requirements

This device is intended for use in the following European Community and EFTA countries:

◆ Austria	◆ Belgium	◆ Bulgaria	◆ Cyprus	◆ Czech Republic
◆ Denmark	◆ Estonia	◆ Finland	◆ France	◆ Germany
◆ Greece	◆ Hungary	◆ Iceland	◆ Ireland	◆ Italy
◆ Latvia	◆ Lithuania	◆ Luxembourg	◆ Malta	◆ Netherlands
◆ Norway	◆ Poland	◆ Portugal	◆ Romania	◆ Slovakia
◆ Slovenia	◆ Spain	◆ Sweden	◆ Switzerland	◆ United Kingdom

NOTE: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

DECLARATION OF CONFORMITY IN LANGUAGES OF THE EUROPEAN COMMUNITY

Czech Česky	Manufacturer tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Estonian Eesti	Käesolevaga kinnitab Manufacturer seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Manufacturer, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish Suomi	Valmistaja Manufacturer vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch Nederlands	Hierbij verklaart Manufacturer dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze Manufacturer dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French Français	Par la présente Manufacturer déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Swedish Svenska	Härmed intygar Manufacturer att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish Dansk	Undertegnede Manufacturer erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF

German Deutsch	Hiermit erklärt Manufacturer, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt Manufacturer die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek Ελληνική	με την παρουσα Manufacturer δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ.
Hungarian Magyar	Alulírott, Manufacturer nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Italian Italiano	Con la presente Manufacturer dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian Latviski	Ar šo Manufacturer deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo Manufacturer deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Maltese Malti	Hawnhekk, Manufacturer, jiddikjara li dan Radio LAN device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Spanish Español	Por medio de la presente Manufacturer declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Polish Polski	Niniejszym Manufacturer oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	Manufacturer declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak Slovensky	Manufacturer týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	Manufacturer izjavlja, da je ta radio LAN device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

About This Guide

Purpose This guide gives specific information on how to install the Wireless-N Access Point/Repeater and its physical and performance related characteristics. It also gives information on how to operate and use the management functions of the Wireless-N Access Point/Repeater.

Audience This guide is for users with a basic working knowledge of computers. You should be familiar with Windows operating system concepts.

Conventions The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications As part of the Wireless-N Access Point/Repeater's software, there is an online web-based help that describes all management related features.

Revision History This section summarizes the changes in each revision of this guide.

January 2010 Revision
This is the first revision of this guide.

CONTENTS

WARRANTY AND PRODUCT REGISTRATION 4

COMPLIANCES 5

ABOUT THIS GUIDE 9

CONTENTS 10

FIGURES 13

TABLES 15

SECTION I GETTING STARTED 16

1 INTRODUCTION 17

Key Hardware Features 17

Description of Capabilities 17

Package Contents 18

Hardware Description 18

LED Indicators 19

Ethernet LAN Ports 20

Power Connector 20

Reset Button 20

WPS Button 20

2 NETWORK PLANNING 21

LAN Access Point 21

Wireless Bridge 22

3 INSTALLING THE ACCESS POINT/REPEATER 23

System Requirements 23

Location Selection 23

Mounting the Device 24

Mounting on a Wall 24

Mounting on a Horizontal Surface 25

4 INITIAL CONFIGURATION 26

Connecting to the Login Page 26
Home Page and Main Menu 27
Common Web Page Buttons 28
Setup Wizard 28
Step 1 - Language Selection 28
Step 2 - Time Settings 29
Step 3 - Wireless Security 29
Completion 30

SECTION II WEB CONFIGURATION 31

5 NETWORK SETTINGS 32

LAN Setting 32

6 WIRELESS CONFIGURATION 34

Basic Settings 34
HT Physical Mode Settings 37
Advanced Settings 38
Advanced Wireless 38
Wi-Fi Multimedia 40
Multicast-to-Unicast Converter 43
WLAN Security 43
Wired Equivalent Privacy (WEP) 44
WPA Pre-Shared Key 46
WPA Enterprise Mode 47
IEEE 802.1X and RADIUS 49
Access Policy 51
Wireless Distribution System (WDS) 51
Wi-Fi Protected Setup (WPS) 54
Station List 56

7 ADMINISTRATION SETTINGS 57

System Management 57
Firmware Upgrade 59
Configuration Settings 60

System Status 61
Statistics 62
System Log 63

SECTION III APPENDICES 65

A TROUBLESHOOTING 66
Diagnosing LED Indicators 66
Before Contacting Technical Support 66

B HARDWARE SPECIFICATIONS 68

C CABLES AND PINOUTS 70
Twisted-Pair Cable Assignments 70
10/100BASE-TX Pin Assignments 71
Straight-Through Wiring 71
Crossover Wiring 72

D LICENSE INFORMATION 73
The GNU General Public License 73

GLOSSARY 77

INDEX 81

FIGURES

Figure 1: Top Panel 18
Figure 2: Rear Panel 19
Figure 3: LEDs 19
Figure 4: Operating as an Access Point 21
Figure 5: Operating as a Wireless Bridge 22
Figure 6: Operating as a Wireless Repeater 22
Figure 7: Wall Mounting 24
Figure 8: Login Page 27
Figure 9: Home Page 27
Figure 10: Wizard Step 1 - Language Selection 28
Figure 11: Wizard Step 2 - Time and SNTP Settings 29
Figure 12: Wizard Step 3 - Wireless Security and Encryption Settings 29
Figure 13: LAN Configuration 32
Figure 14: Basic Settings 35
Figure 15: HT Physical Mode Settings 37
Figure 16: Advanced Wireless Settings 38
Figure 17: Wi-Fi Multimedia Settings 41
Figure 18: WMM Configuration 42
Figure 19: Multicast-to-Unicast Converter 43
Figure 20: Security Mode Options 44
Figure 21: Security Mode - WEP 45
Figure 22: Security Mode - WPA-PSK 46
Figure 23: Security Mode - WPA 48
Figure 24: Security Mode - 802.1X 50
Figure 25: Access Policy 51
Figure 26: Manual WDS MAC Address Configuration 52
Figure 27: WDS Configuration Example 52
Figure 28: WDS Configuration 53
Figure 29: Enabling WPS 54
Figure 30: WPS Configuration 55
Figure 31: Station List 56

Figure 32: System Management 57
Figure 33: Time Zone Settings 58
Figure 34: Firmware Upgrade 59
Figure 35: Configuration Settings 60
Figure 36: System Status 61
Figure 37: Statistics 62
Figure 38: System Log 63
Figure 39: RJ-45 Connector 70
Figure 40: Straight-through Wiring 72
Figure 41: Crossover Wiring 72

TABLES

Table 1: Key Hardware Features 17
Table 2: LED Behavior 19
Table 3: WMM Access Categories 41
Table 4: LED Indicators 66
Table 5: 10/100BASE-TX MDI and MDI-X Port Pinouts 71

SECTION I

GETTING STARTED

This section provides an overview of the Wireless-N Access Point/Repeater, and describes how to install and mount the unit. It also describes the basic settings required to access the management interface and run the setup Wizard.

This section includes these chapters:

- "Introduction" on page 17
- "Network Planning" on page 24
- "Installing the Access Point/Repeater" on page 25
- "Initial Configuration" on page 28

1 INTRODUCTION

The Wireless-N Access Point/Repeater (SMCWEBS-N) supports an access point service that extends a local wired network to wireless clients. It is simple to configure and can be up and running in minutes.

KEY HARDWARE FEATURES

The following table describes the main hardware features of the Access Point/Repeater.

Table 1: Key Hardware Features

Feature	Description
4 LAN Ports	Four 100BASE-TX RJ-45 ports for local network connections.
WPS Button	To set up a secure connection to a wireless device.
Reset Button	For resetting the unit and restoring factory defaults.
LEDs	Provides LED indicators for Power, LAN ports, WLAN, and WPS status.
Mounting Options	Can be mounted on any horizontal surface such as a desktop or shelf, or on a wall using two screws.

DESCRIPTION OF CAPABILITIES

- Local network connection through four 10/100 Mbps Ethernet ports, making it easy to create a network in small offices or homes.
- Easy setup through a Web browser on any operating system that supports TCP/IP.
- Compatible with all popular Internet applications.
- The Access Point/Repeater supports security features that provides WPA (Wi-Fi Protected Access) and MAC filtering provide security over the wireless network.

PACKAGE CONTENTS

The Wireless-N Access Point/Repeater package includes:

- Wireless-N Access Point/Repeater (SMCWEBS-N)
- RJ-45 Category 5 network cable
- AC power adapter
- SMC Warranty Information Card
- Quick Installation Guide

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

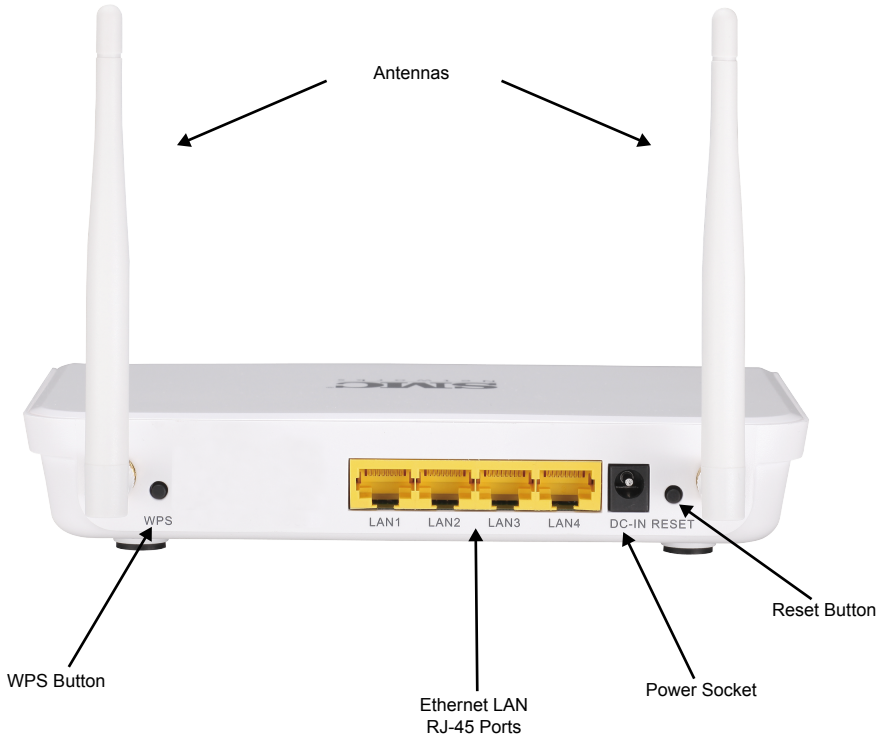
HARDWARE DESCRIPTION

The Wireless-N Access Point/Repeater, from herein refered to as Access Point/Repeater, connects to your PC or to a local area network using its RJ-45 Fast Ethernet LAN ports.

The Access Point/Repeater includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting.

Figure 1: Top Panel

Figure 2: Rear Panel



LED INDICATORS

The Wireless-N Access Point/Repeater includes seven status LED indicators, as described in the following figure and table.

Figure 3: LEDs

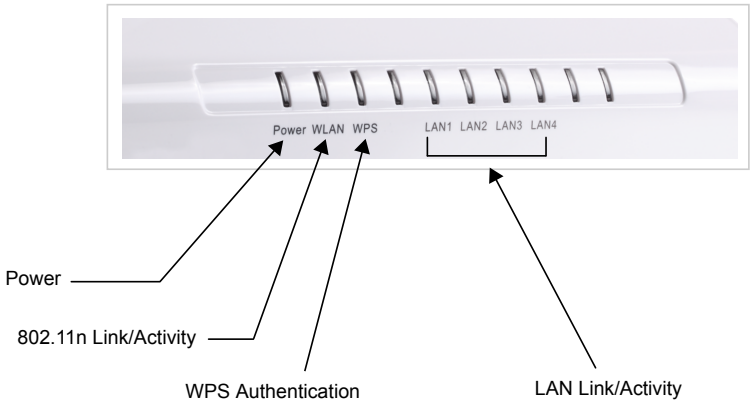


Table 2: LED Behavior

LED	Status	Description
Power	On Blue	The unit is receiving power and is operating normally.
	Off	There is no power currently being supplied to the unit.

Table 2: LED Behavior (Continued)

LED	Status	Description
WLAN	On/Blinking Blue	The 802.11n radio is enabled and transmitting or receiving data through wireless links.
	Off	The 802.11n radio is disabled.
WPS	Blinking	WPS authentication is in progress.
	Off	WPS authentication is not in progress.
LAN1~LAN4	On Blue	The Ethernet LAN port is connected to a PC or server.
	Blinking	The Ethernet port is connected and is transmitting/receiving data.
	Off	The Ethernet port is disconnected or has malfunctioned.

ETHERNET LAN PORTS

The Wireless-N Access Point/Repeater has four 100BASE-TX RJ-45 ports that can be attached directly to 10BASE-T/100BASE-TX LAN segments.

These port support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

POWER CONNECTOR

The Wireless-N Access Point/Repeater must be powered with its supplied power adapter. Failure to do so results in voiding of any warrantly supplied with the product. The power adapter automatically adjusts to any voltage between 100~240 volts at 50 or 60 Hz, and supplies 5 volts DC power to the unit. No voltage range settings are required.

RESET BUTTON

This button is used to restore the factory default configuration. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the Access Point/Repeater.

WPS BUTTON

Press to automatically configure the Wireless-N Access Point/Repeater with other WPS devices in the WLAN.

2 NETWORK PLANNING

The Wireless-N Access Point/Repeater is designed as an access point that extends an existing wired network to support wireless users. It also supports use as a wireless repeater/bridge that can extend the range of the network or connect to remote LANs.

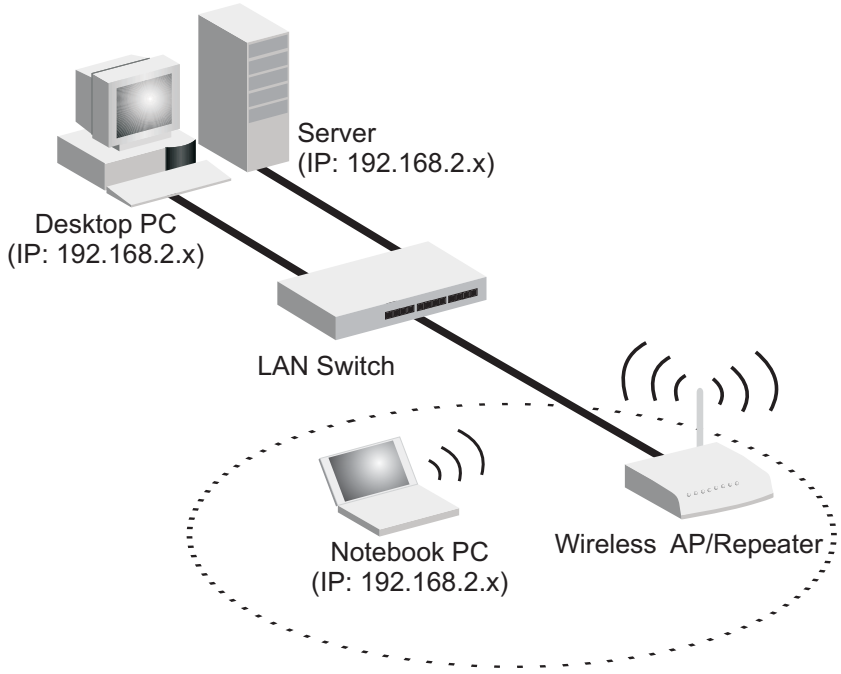
This chapter explains some of the basic features of the Wireless-N Access Point/Repeater and shows some network topology examples in which the device is implemented.

LAN ACCESS POINT

The Wireless-N Access Point/Repeater can provide an access point service for an existing wired LAN, creating a wireless extension to the local network.

A Wi-Fi wireless network is defined by its Service Set Identifier (SSID) or network name. Wireless clients that want to connect to a network must set their SSID to the same SSID of the network service.

Figure 4: Operating as an Access Point



WIRELESS BRIDGE

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for bridge connections between access points. The Wireless-N Access Point/Repeater can use WDS to forward traffic on links between units.

Up to four WDS links can be specified for the Wireless-N Access Point/ Repeater.

The WDS feature enables two basic functions to be configured in the wireless network. Either a repeater function that extends the range of the wireless network, or a bridge function that connects a remote LAN segment to an Internet connection.

Figure 5: Operating as a Wireless Bridge

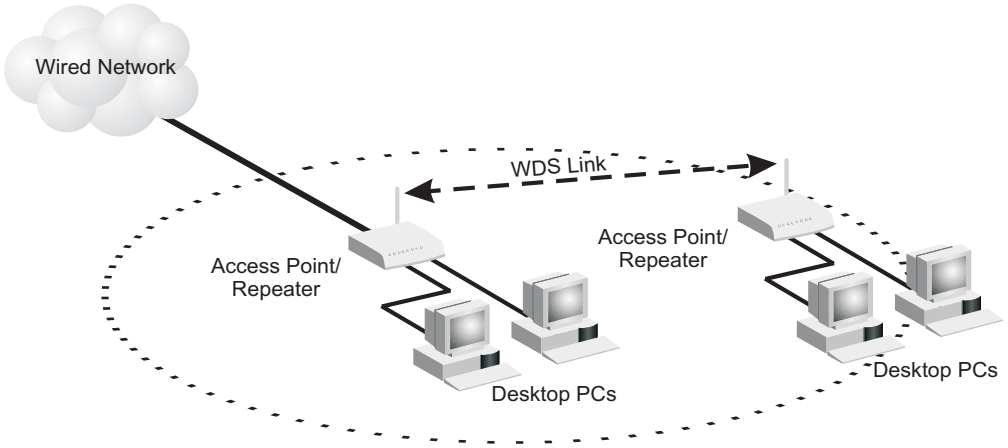
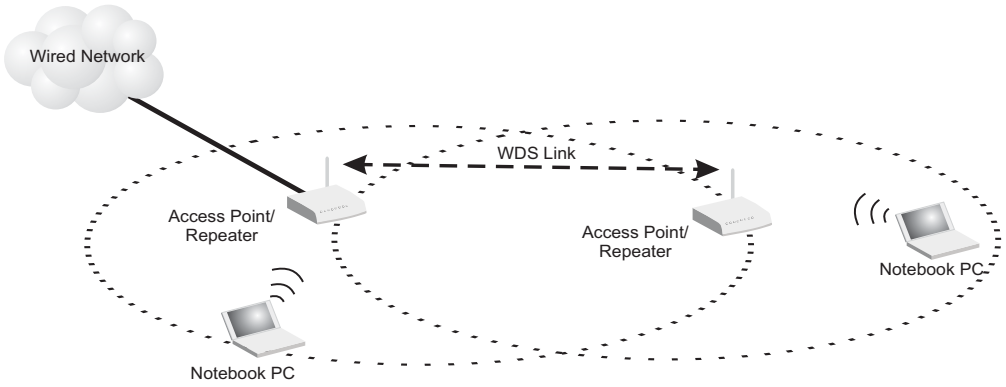


Figure 6: Operating as a Wireless Repeater



3 Installing the Access Point/ Repeater

This chapter describes how to install the access point.

System Requirements

You must meet the following minimum requirements:

- An Internet access device (DSL or Cable modem) with an Ethernet port connection.
- An up-to-date web browser: Internet Explorer 6.0 or above or Mozilla Firefox 2.0 or above.

Location Selection

Choose a proper place for the access point/repeater. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. Try to place the access point in a position that can best cover its service area. For optimum performance, consider these guidelines:

- Mount the access point as high as possible above any obstructions in the coverage area.
- Avoid mounting next to or near building support columns or other obstructions that may cause reduced signal or null zones in parts of the coverage area.
- Mount away from any signal absorbing or reflecting structures (such as those containing metal).The access point can be mounted on any horizontal surface, or a wall.

MOUNTING THE DEVICE

The Wireless-N Access Point/Repeater can be mounted on any horizontal surface, or on a wall. The following sections describe the mounting options.

MOUNTING ON A WALL

The Wireless-N Access Point/Repeater should be mounted only to a wall or wood surface that is at least 1/2-inch plywood or its equivalent. To mount the unit on a wall, always use its wall-mounting slots. The unit must be mounted with the RJ-45 cable connector oriented upwards to ensure proper operation.

Figure 7: Wall Mounting

To mount on a wall, follow the instructions below.

1. Mark the position of the two screw holes on the wall. For concrete or brick walls, you will need to drill holes and insert wall plugs for the screws.

2. Insert two 20-mm M4 tap screws (not included) into the holes, leaving about 2~3 mm (0.08~0.12 inches) clearance from the wall.

3. Line up the two mounting points on the unit with the screws in the wall, then slide the unit down onto the screws until it is in a secured position.

MOUNTING ON A HORIZONTAL SURFACE

To keep the Wireless-N Access Point/Repeater from sliding on the surface, the Wireless-N Access Point/Repeater has four rubber feet on the bottom of the unit.

It is recommended to select an uncluttered area on a sturdy surface, such as a desktop or table. The unit can also be protected by securing all attached cables to a table leg or other nearby fixed structure.

4 INITIAL CONFIGURATION

The Wireless-N Access Point/RepeaterWireless-N Access Point/Repeater offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

CONNECTING TO THE LOGIN PAGE

It is recommended to make initial configuration changes by connecting a PC directly to one of the Wireless-N Access Point/Repeater's LAN ports. The Wireless-N Access Point/Repeater has a default IP address of 192.168.2.10 and a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the Access Point/Repeater (that is, the PC and Access Point/Repeater addresses must both start 192.168.2.x).

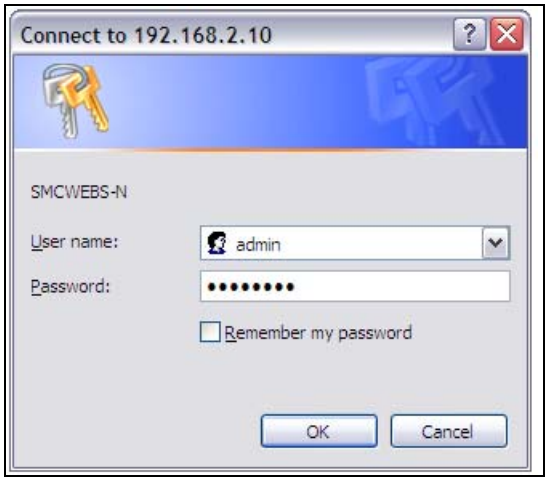
To access the Wireless-N Access Point/Repeater's management interface, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.10.

2. Log into the interface by entering the default username "admin" and password "smcadmin," then click Login.

NOTE: It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, See "System Management" on page 64.

Figure 8: Login Page



HOME PAGE AND MAIN MENU

After logging in to the web interface, the Home page displays. The Home page shows the main menu and the method to access the Setup Wizard.

Figure 9: Home Page

COMMON WEB PAGE BUTTONS

The list below describes the common buttons found on most web management pages:

- **Apply** – Applies the new parameters and saves them to memory. Also displays a screen to inform you when it has taken affect. Clicking 'Apply' returns to the home page.
- **Cancel** – Cancels the newly entered settings and restores the previous settings.
- **Next** – Proceeds to the next step.
- **Previous** – Returns to the previous screen.

SETUP WIZARD

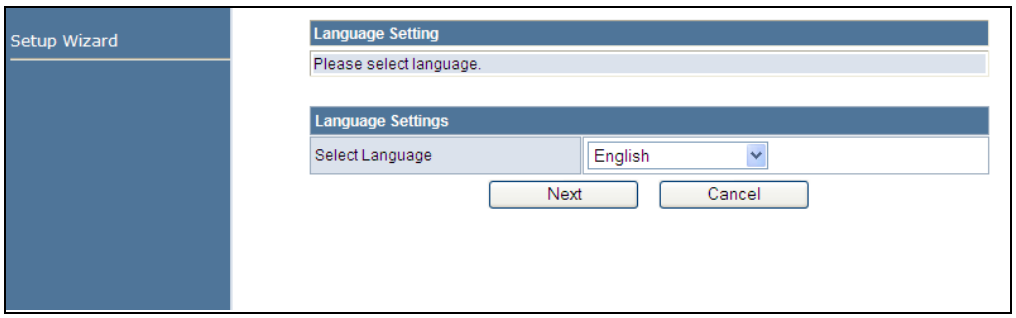
The Wizard is designed to help you configure the basic settings required to get the the Wireless-N Access Point/Repeater up and running. There are only a few basic steps you need to set up the the Wireless-N Access Point/ Repeater and provide a connection.

Follow these steps:

STEP 1 - LANGUAGE SELECTION

Select between English, Traditional Chinese, Simple Chinese, or Korean. Click Next to proceed to the next step of the wizard.

Figure 10: Wizard Step 1 - Language Selection



The following items are displayed on the first page of the Setup Wizard:

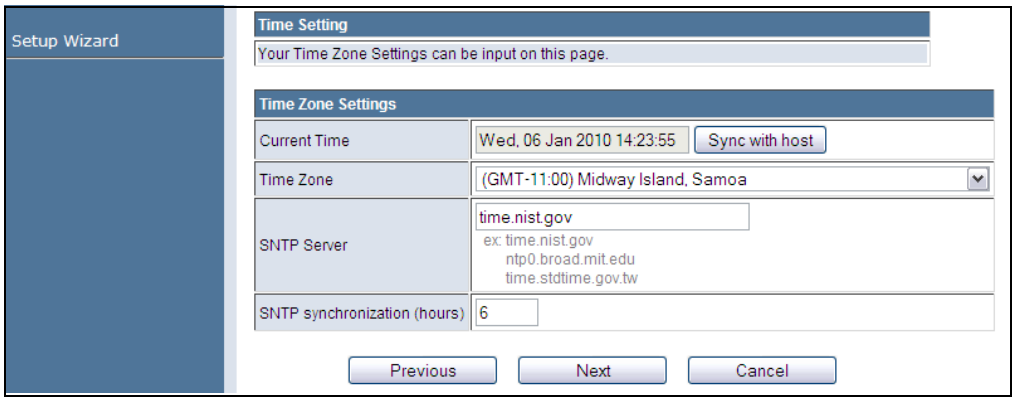
- **Select Language** — Selects English, Traditional Chinese, Simple Chinese, or Korean as the interface language.

STEP 2 - TIME SETTINGS

The Step 2 page of the Wizard configures time zone and SNTP settings.

Select a time zone according to where the device is operated. Click Next after completing the setup.

Figure 11: Wizard Step 2 - Time and SNTP Settings



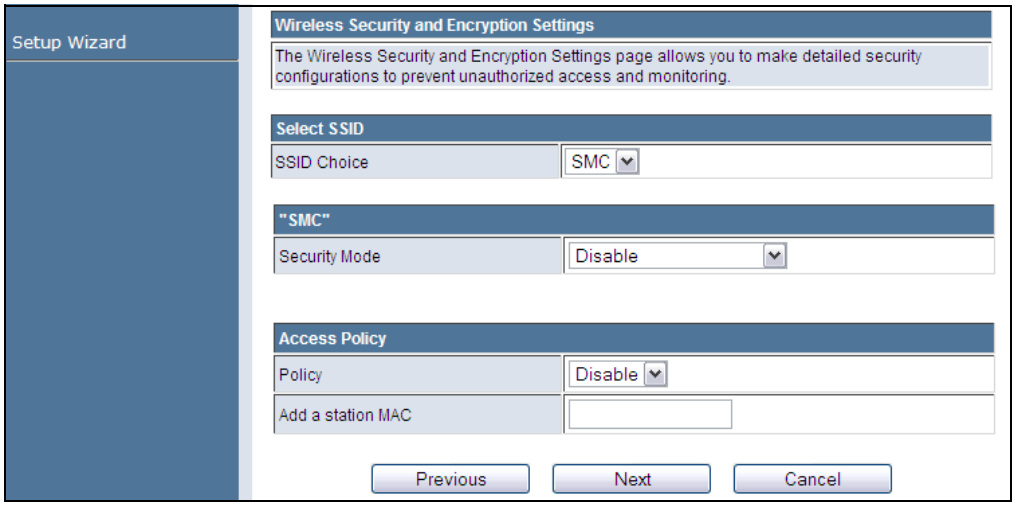
The following items are displayed on this page:

- **Current Time** — Receives a time and date stamp from an SNTP server.
- **Time Zone** — Select the time zone that is applicable to your region.
- **SNTP Server** — Enter the address of an SNTP server to receive time updates.
- **SNTP synchronization (hours)** — Specify the interval between SNTP server updates.

STEP 3 - WIRELESS SECURITY

The Step 3 page of the Wizard configures the wireless network name and security options.

Figure 12: Wizard Step 3 - Wireless Security and Encryption Settings



The following items are displayed on this page:

- **SSID Choice** — The name of the wireless network service provided by the Wireless-N Access Point/Repeater. Clients that want to connect to the network must set their SSID to the same as that of the Wireless-N Access Point/Repeater. (Default: "SMC")

- **Security Mode** — Specifies the security mode for the SSID. Select the security method and then configure the required parameters. For more information, see "WLAN Security" on page 43. (Options: Disabled, Open, Shared, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK, WPA, WPA2, WPA1_WPA2, 802.1X; Default: Disabled)

NOTE: To keep your wireless network protected and secure, you should implement the highest security possible. For small networks, it is recommended to select WPA2-PSK using AES encryption as the most secure option. However, if you have older wireless devices in the network that do not support AES encryption, select TKIP as the encryption algorithm.

- **Access Policy** — The Wireless-N Access Point/Repeater provides a MAC address filtering facility. The access policy can be set to allow or reject specific station MAC addresses. This feature can be used to connect known wireless devices that may not be able to support the configured security mode.

- **Add a station MAC —** Enter the MAC address of the station that you want to filter. MAC addresses must be entered in the format xx:xx:xx:xx:xx:xx.

COMPLETION After completion of the Wizard, the screen returns to the Home Page.

SECTION II

WEB CONFIGURATION

This section provides details on configuring the Wireless-N Access Point/ Repeater using the web browser interface.

This section includes these chapters:

- "Network Settings" on page 32
- "Wireless Configuration" on page 34
- "Administration Settings" on page 57

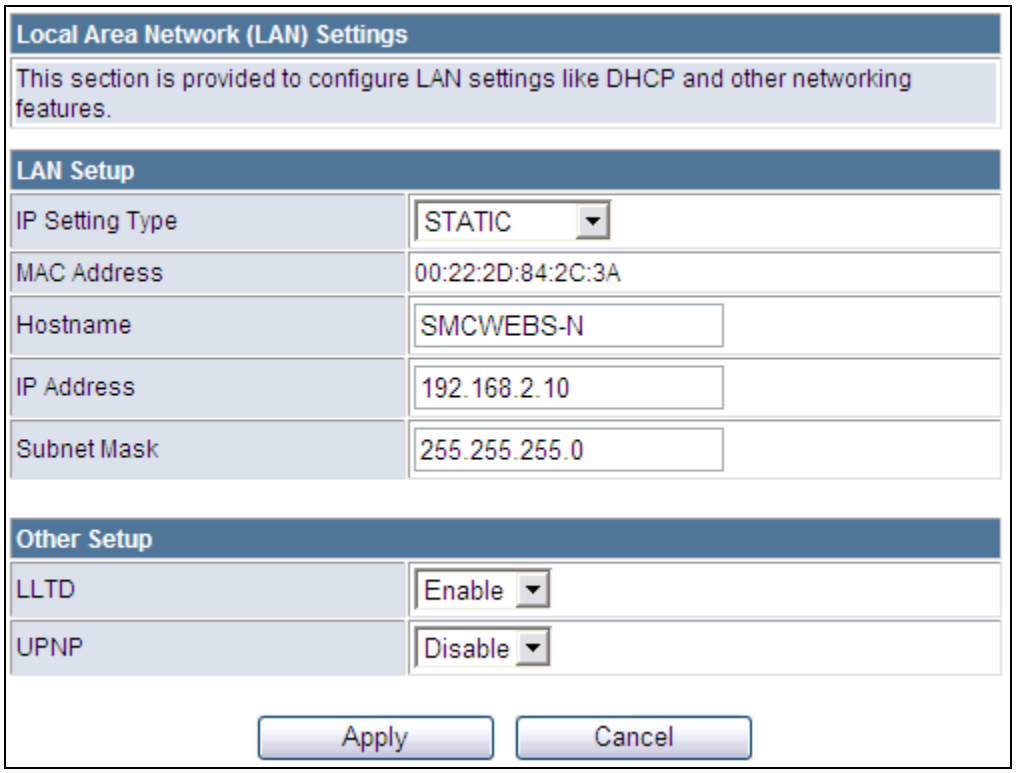
5 NETWORK SETTINGS

The Network Settings pages allow you to manage basic system configuration settings.

LAN SETTING

The Wireless-N Access Point/Repeater must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.2.10. You can use this IP address or assign another address that is compatible with your existing local network. Click on “Network Settings” followed by “LAN.”

Figure 13: LAN Configuration



The following items are displayed on this page:

- **IP Setting Type** — By default, the access point WAN port is configured with DHCP enabled. After you have network access to the access point, you can use the web browser interface to modify the initial IP configuration, if needed. (Options: STATIC and DHCP; Default: DHCP).

- **MAC Address** — The shared physical layer address for the Wireless-N Access Point/Repeater's LAN ports.
- **Hostname** — The hostname of the STATIC or DHCP client.
- **IP Address** — Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.2.10.
- **Subnet Mask** — Indicate the local subnet mask. (Default: 255.255.255.0.)
- **LLTD** — Link Layer Topology Discovery (LLTD) is a Microsoft proprietary discovery protocol which can be used for both wired and wireless networks. (Options: Disable/Enable, Default: Enabled)
- **UPNP** — Allows the device to advertise its UPnP capabilities. (Default: Disabled)

6 WIRELESS CONFIGURATION

The wireless settings section displays configuration settings for the access point functionality of the Wireless-N Access Point/Repeater. It includes the following sections:

- "Basic Settings" on page 34
- "Advanced Settings" on page 38
- "WLAN Security" on page 43
- "Wireless Distribution System (WDS)" on page 51
- "Wi-Fi Protected Setup (WPS)" on page 54
- "Station List" on page 56

BASIC SETTINGS

The IEEE 802.11n interface includes configuration options for radio signal characteristics and wireless security features.

The Wireless-N Access Point/Repeater's radio can operate in six modes, mixed 802.11b/g/n, mixed 802.11b/g, mixed 802.11g/n, 802.11n only, 802.11b only, or 802.11g only. Note that 802.11g is backward compatible with 802.11b, and 802.11n is backward compatible with 802.11b/g at slower data transmit rates.

The Wireless-N Access Point/Repeater supports four virtual access point (VAP) interfaces. One VAP is the primary (Network Name SSID), and the the others are referred to as "Multiple SSID1~SSID3." Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces.

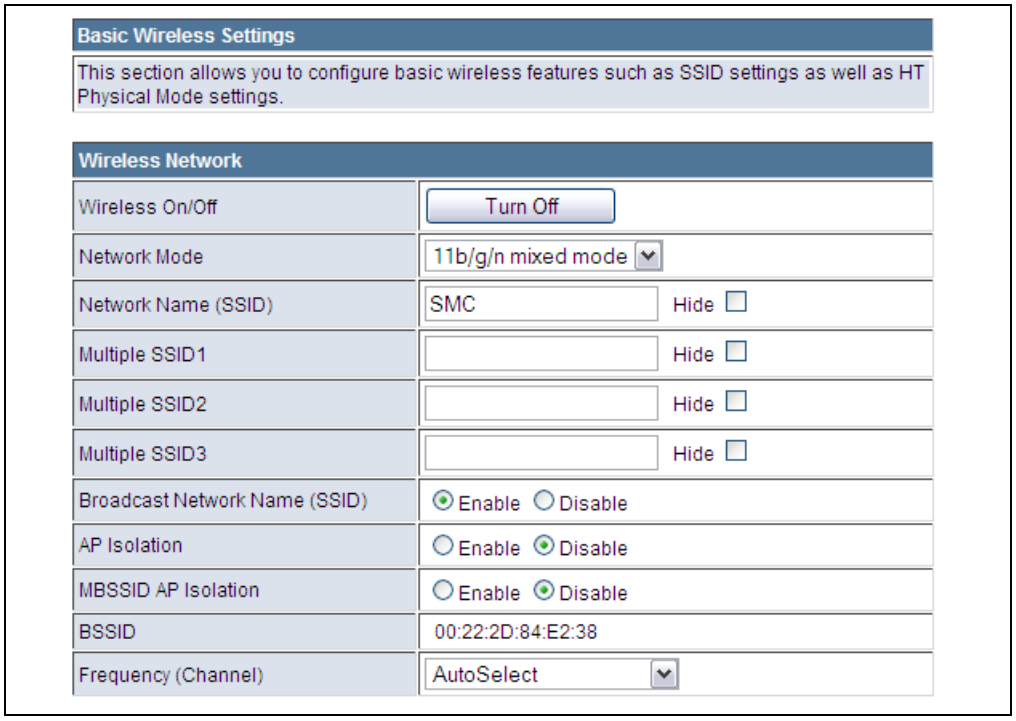
Traffic to specific VAPs can be segregated based on user groups or application traffic. All VAPs can have up to 64 wireless clients, whereby the clients associate with these VAPs the same as they would with a physical access point.

NOTE: The radio channel settings for the access point are limited by local regulations, which determine the number of channels that are available.

The Basic Settings page allows you to configure the wireless network name (Service Set Identifier or SSID) and set the wireless security method.

Click on "Wireless Settings," followed by "Basic."

Figure 14: Basic Settings



The following items are displayed on this page:

- **Wireless On/Off** — Enables or Disable the radio. (Default: Enable)
- **Network Mode** — Defines the radio operating mode. (Default: 11g/n Mixed)
  - **11b/g mixed mode**: Both 802.11b and 802.11g clients can communicate with the Wireless-N Access Point/Repeater (up to 108 Mbps), but data transmission rates may be slowed to compensate for 802.11b clients. Any 802.11n clients will also be able to communicate with the Wireless-N Access Point/Repeater, but they will be limited to 802.11g protocols and data transmission rates.
  - **11b only**: All 802.11b, 802.11g, and 802.11n clients will be able to communicate with the Wireless-N Access Point/Repeater, but the 802.11g and 802.11n clients will be limited to 802.11b protocols and data transmission rates (up to 11 Mbps).
  - **11g only**: Both 802.11g and 802.11n clients will be able to communicate with the Wireless-N Access Point/Repeater, but the 802.11n clients will be limited to 802.11g protocols and data transmission rates (up to 54 Mbps). Any 802.11b clients will not be able to communicate with the Wireless-N Access Point/Repeater.

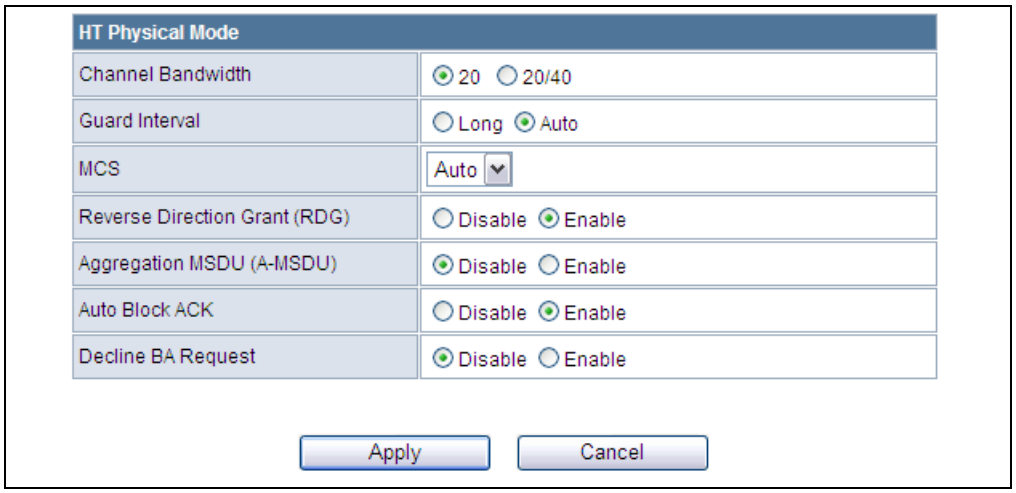
- **11b/g/n mixed mode**: All 802.11b/g/n clients can communicate with the Wireless-N Access Point/Repeater (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11b/g clients.
- **11n only**: Only 802.11n clients will be able to communicate with the Wireless-N Access Point/Repeater (up to 150 Mbps).
- **11g/n mixed mode**: Both 802.11g and 802.11n clients can communicate with the Wireless-N Access Point/Repeater (up to 150 Mbps), but data transmission rates may be slowed to compensate for 802.11g clients.

- **Network Name (SSID)** — The name of the wireless network service provided by the Wireless-N Access Point/Repeater. Clients that want to connect to the network must set their SSID to the same as that of the Wireless-N Access Point/Repeater. (Default: "SMC"; Range: 1-32 characters)
- **Multiple SSID1~SSID3** — Three additional VAP interface supported on the device. (Default: no name configured; Range: 1-32 characters)
- **Broadcast Network Name (SSID)** — By default, the Wireless-N Access Point/Repeater always broadcasts the SSID in its beacon signal. Disabling the SSID broadcast increases security of the network because wireless clients need to already know the SSID before attempting to connect. When set to disable, the Network Name SSID, and SSID1~SSID3 are automatically set to "Hide." (Default: Enabled)
- **AP Isolation** — The Wireless-N Access Point/Repeater will isolate communincation between all clients in order to protect them. Normally for users who are at hotspots. (Default: Disabled)
- **MBSSID AP Isolation** — The Wireless-N Access Point/Repeater will isolate wireless clients from different SSID. (Default: Disabled)
- **BSSID** — The identifier (MAC address) of the Wireless-N Access Point/Repeater in the Basic Service Set (BSS) network.
- **Frequency (Channel)** — The radio channel that the Wireless-N Access Point/Repeater uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the Wireless-N Access Point/Repeater to which it is linked. Selecting Auto Select enables the Wireless-N Access Point/Repeater to automatically select an unoccupied radio channel. (Default: AutoSelect)

HT PHYSICAL MODE SETTINGS

The HT Physical Mode section on the Wireless Settings Advanced page includes additional parameters for 802.11n operation.

Figure 15: HT Physical Mode Settings



The following items are displayed in this section on this page:

- **Channel Bandwidth** — The Wireless-N Access Point/Repeater provides a channel bandwidth of 40 MHz by default giving an 802.11g connection speed of 108 Mbps (sometimes referred to as Turbo Mode) and a 802.11n connection speed of up to 150 Mbps. Setting the HT Channel Bandwidth to 20 MHz slows connection speed for 802.11g and 802.11n to 54 Mbps and 74 Mbps respectively and ensures backward compliance for slower 802.11b devices. (Default: 20MHz)

- **Guard Interval** — The guard interval between symbols helps receivers overcome the effects of multipath delays. When you add a guard time, the back portion of useful signal time is copied and appended to the front. (Default: Auto)

- **MCS** — The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels. (Options: value [range] = 0~7 (1 Tx Stream), 8~15 (2 TxStream), 32 and auto (33). Default: Auto)

- **Reverse Direction Grant (RDG)** — When Reverse Direction Grant is enabled, the Wireless-N Access Point/Repeater can reduce the transmitted data packet collision by using the reverse direction protocol. During TXOP (Transmission Opportunity) period, the receiver could use remaining transmission time to transmit data to a sender. The RDG improves transmission performance and scalability in a wireless environment. (Default: Enabled)

- **Aggregate MSDU (A-MSDU)** — This option enables Mac Service Data Unit (MSDU) aggregation. (Default: Disabled)

- **Auto Block ACK** — Select to block ACK (Acknowledge Number) or not during data transferring. (Default: Enabled)

- **Decline BA Request** — Select to reject peer BA-Request or not. (Default: Disabled)

ADVANCED SETTINGS

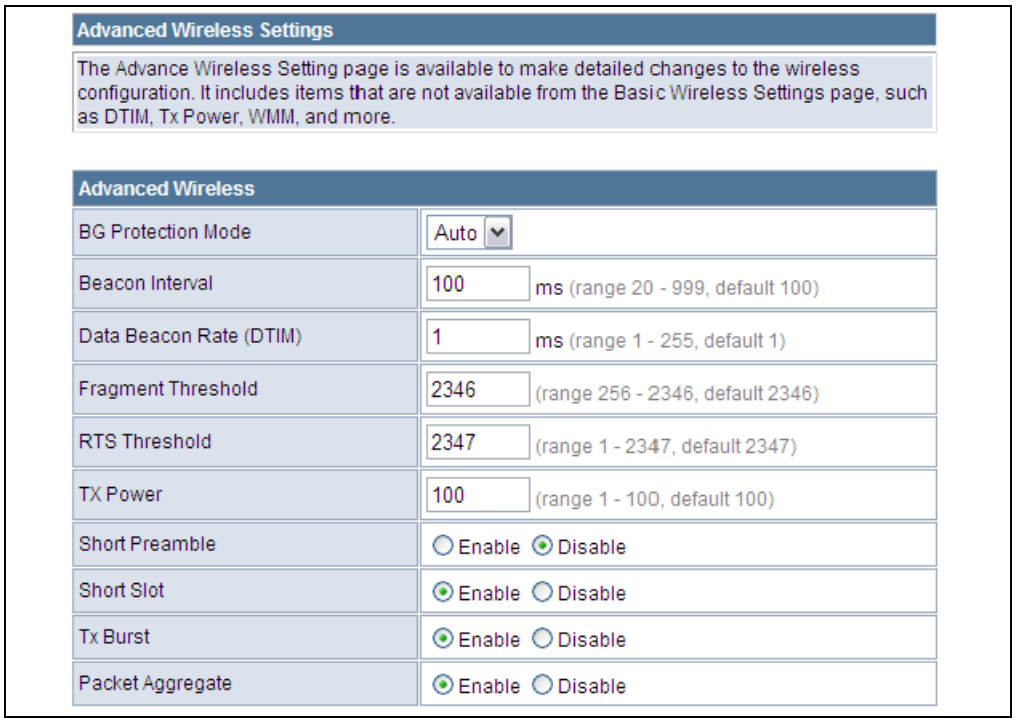
The Advanced Settings page includes additional parameters concerning the wireless network and Wi-Fi Multimedia settings.

NOTE: There are several variables to consider when selecting a radio mode that make it fully functional. Simply selecting the mode you want is not enough to ensure full compatibility for that mode. Information on these variables may be found in the HT Physcial Mode Setting section.

ADVANCED WIRELESS

The Advanced Wireless section on the Wireless Settings Advanced page includes additional radio parameters.

Figure 16: Advanced Wireless Settings



The following items are displayed in this section on this page:

- **BG Protection Mode** — Enables a backward compatible protection mechanism for 802.11b clients. There are three modes: (Default: Auto)
  - **Auto** — The unit enables its protection mechanism for 802.11b clients when they are detected in the network. When 802.11b clients are not detected, the protection mechanism is disabled.
  - **On** — Forces the unit to always use protection for 802.11b clients, whether they are detected in the network or not. Note that enabling b/g Protection can slow throughput for 802.11g/n clients by as much as 50%.
  - **Off** — Forces the unit to never use protection for 802.11b clients. This prevents 802.11b clients from connecting to the network.
- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They may also carry power-management information. (Range: 20-999 TUs; Default: 100 TUs)
- **Data Beacon Rate (DTIM)** — The rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions.

  Known also as the Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of one beacon indicates that the access point will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every beacon. Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames. (Range: 1-255 beacons; Default: 1 beacon)
- **Fragmentation Threshold** – Configures the minimum packet size that can be fragmented when passing through the access point. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Range: 256-2346 bytes; Default: 2346 bytes)
- **RTS Threshold** — Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame.

After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled.

The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Range: 1-2347 bytes: Default: 2347 bytes)

- **TX Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area.

- **Short Preamble** — Sets the length of the signal preamble that is used at the start of a data transmission. Use a short preamble (96 microseconds) to increase data throughput when it is supported by all connected 802.11g clients. Use a long preamble (192 microseconds) to ensure all 802.11b clients can connect to the network. (Default: Disabled)

- **Short Slot** — Sets the basic unit of time the access point uses for calculating waiting times before data is transmitted. A short slot time (9 microseconds) can increase data throughput on the access point, but requires that all clients can support a short slot time (that is, 802.11g-compliant clients must support a short slot time). A long slot time (20 microseconds) is required if the access point has to support 802.11b clients. (Default: Enabled)

- **TX Burst** — A performance enhancement that transmits a number of data packets at the same time when the feature is supported by compatible clients. (Default: Enabled)

- **Packet Aggregate** — A performance enhancement that combines data packets together when the feature is supported by compatible clients. (Default: Enabled)

WI-FI MULTIMEDIA

The Wireless-N Access Point/Repeater implements Quality of Service (QoS) using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the developing IEEE 802.11e QoS standard and it enables access points to interoperate with both WMM-enabled clients and other devices that may lack any WMM functionality.

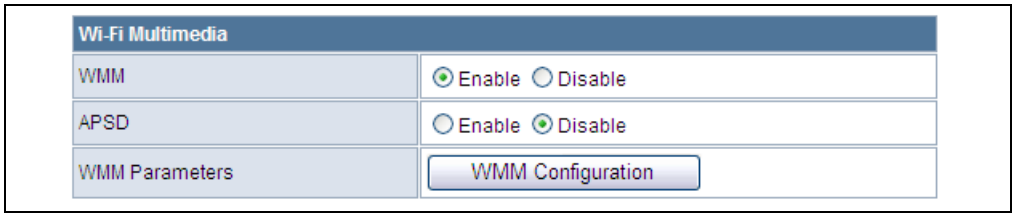
WMM defines four access categories (ACs): voice, video, best effort, and background. These categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags (see Table 3). The direct mapping of the four ACs to 802.1D priorities is specifically intended to facilitate interoperability with other wired network QoS policies. While the four ACs are specified for specific types of traffic, WMM allows the priority levels to be configured to match any network-wide QoS policy. WMM also specifies a protocol that access points can use to communicate the configured traffic priority levels to QoS-enabled wireless clients.

Table 3: WMM Access Categories

Access Category	WMM Designation	Description	802.1D Tags
AC_VO (AC3)	Voice	Highest priority, minimum delay. Time-sensitive data such as VoIP (Voice over IP) calls.	7, 6
AC_VI (AC2)	Video	High priority, minimum delay. Time-sensitive data such as streaming video.	5, 4
AC_BE (AC0)	Best Effort	Normal priority, medium delay and throughput. Data only affected by long delays. Data from applications or devices that lack QoS capabilities.	0, 3
AC_BK (AC1)	Background	Lowest priority. Data with no delay or throughput requirements, such as bulk data transfers.	2, 1

The Wi-Fi Multimedia section on the Wireless Settings Advanced page allows you to enable WMM and set detailed QoS parameters.

Figure 17: Wi-Fi Multimedia Settings



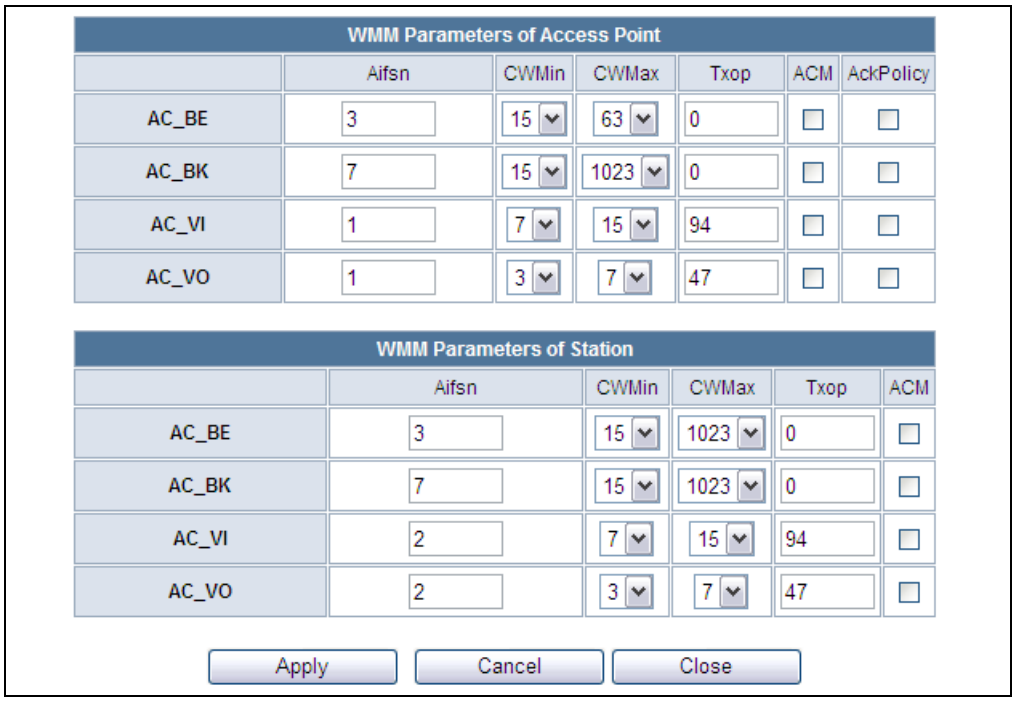
The following items are displayed in this section on this page:

- **WMM** — Sets the WMM operational mode on the access point. When enabled, the QoS capabilities are advertised to WMM-enabled clients in the network. WMM must be supported on any device trying to associated with the access point. Devices that do not support this feature will not be allowed to associate with the access point. (Default: Enabled)

- **APSD** — When WMM is enabled, Automatic Power Save Delivery (APSD) can also be enabled. APSD is an efficient power management method that enables client devices sending WMM packets to enter a low-power sleep state between receiving and transmitting data. (Default: Disabled)

- **WMM Parameters** — Click the WMM Configuration button to set detailed WMM parameters.

Figure 18: WMM Configuration



The following items are displayed in the WMM Configuration window:

- **AIFSN** (Arbitration Inter-Frame Space) — The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

- **CWMin** (Minimum Contention Window) — The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.

- **CWMax** (Maximum Contention Window) — The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.

- **Txop** (Transmit Opportunity Limit) — The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TxOpLimit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-65535 microseconds.

- **ACM** — The admission control mode for the access category. When enabled, clients are blocked from using the access category. (Default: Disabled)
- **AckPolicy** — By default, all wireless data transmissions require the sender to wait for an acknowledgement from the receiver. WMM allows the acknowledgement wait time to be turned off for each Access Category (AC) 0-3. Although this increases data throughput, it can also result in a high number of errors when traffic levels are heavy. (Default: Acknowledge)

MULTICAST-TO-UNICAST CONVERTER

The Multicast-to-Unicast Converter section on the Wireless Settings Advanced page allows you to enable multicast traffic conversion.

Converting multicast traffic to unicast before sending to wireless clients allows a longer DTIM (Data Beacon Rate) interval to be set. A longer DTIM interval prevents clients in power-save mode having to activate their radios to receive the multicast data, which saves battery life.

Figure 19: Multicast-to-Unicast Converter

The following items are displayed in this section on this page:

- **Multicast-to-Unicast** — Enables multicast traffic streams to be converted to unicast traffic before delivery to wireless clients. (Default: Disabled)

WLAN SECURITY

The Wireless-N Access Point/Repeater's wireless interface is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with a configured SSID of "ANY" can read the SSID from the beacon, and automatically set their SSID to allow immediate connection to the wireless network.

To implement wireless network security, you have to employ one or both of the following functions:

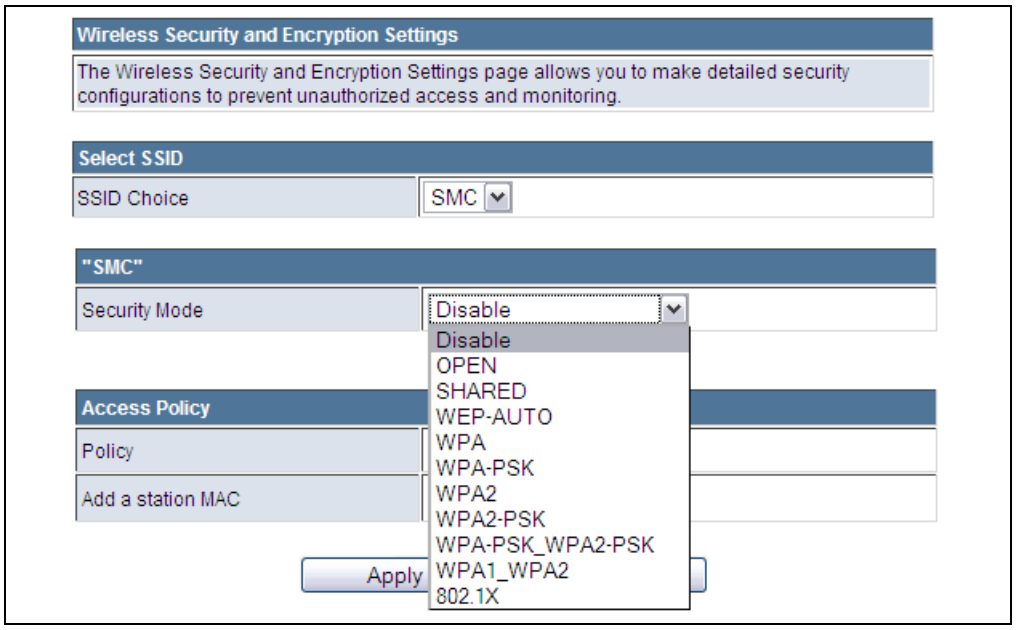
- **Authentication** — It must be verified that clients attempting to connect to the network are authorized users.
- **Traffic Encryption** — Data passing between the unit and clients must be protected from interception and eavesdropping.

The Wireless-N Access Point/Repeater supports supports ten different security mechanisms that provide various levels of authentication and encryption depending on the requirements of the network.

The Wireless-N Access Point/Repeater supports four SSID interfaces. Each SSID interface functions as a separate access point, and can be configured with its own security settings.

Click on “Wireless Settings,” followed by “Basic”.

Figure 20: Security Mode Options



The supported security mechanisms and their configuration parameters are described in the following sections:

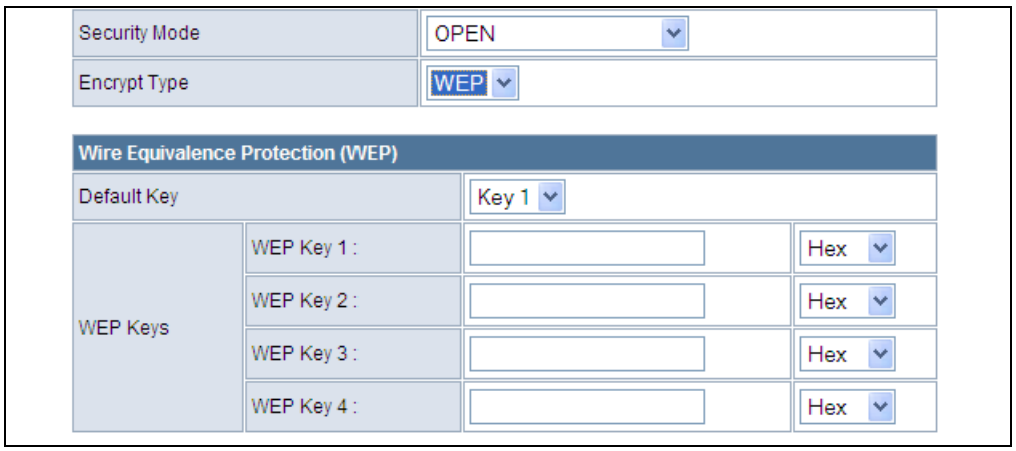
- **OPEN, SHARED, WEP-AUTO** — See “Wired Equivalent Privacy (WEP)” on page 44
- **WPA-PSK, WPA2-PSK, WPA-PSK_WPA2-PSK** — See “WPA Pre-Shared Key” on page 46
- **WPA, WPA2, WPA1_WPA2** — See “WPA Enterprise Mode” on page 47
- **802.1X** — See “IEEE 802.1X and RADIUS” on page 49

WIRED EQUIVALENT PRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

Figure 21: Security Mode - WEP



The following items are displayed in this section on this page:

Security Mode — Configures the WEP security mode used by clients. When using WEP, be sure to define at least one static WEP key for the Wireless-N Access Point/Repeater and all its clients. (Default: Disable)

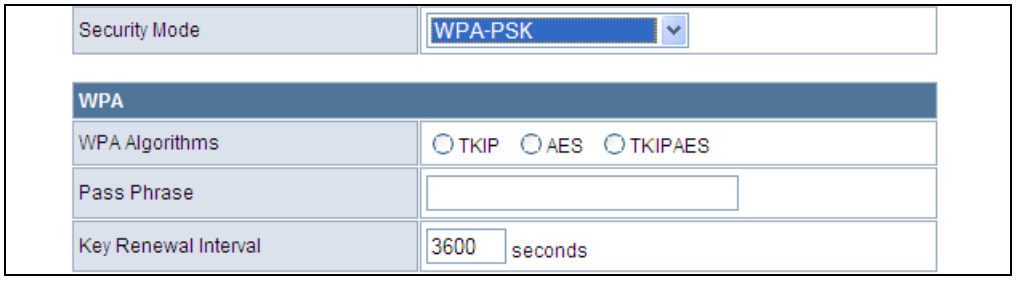
- **OPEN** — Open-system authentication accepts any client attempting to connect the Wireless-N Access Point/Repeater without verifying its identity. In this mode the default data encryption type is "WEP."
- **SHARED** — The shared-key security uses a WEP key to authenticate clients connecting to the network and for data encryption.
- **WEP-AUTO** — Allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).
- **Encrypt Type** — Selects WEP for data encryption (OPEN mode only).
- **Default Key** — Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys. (Default: 1; Range: 1~4)
- **WEP Keys 1 ~ 4** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

WPA PRE-SHARED KEY

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an "enterprise" and "personal" mode of operation.

For small home or office networks, WPA and WPA2 provide a simple "personal" operating mode that uses just a pre-shared key for network access. The WPA Pre-Shared Key (WPA-PSK) mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.

Figure 22: Security Mode - WPA-PSK



The following items are displayed in this section on this page:

Security Mode — Configures the WPA-PSK and WPA2-PSK security modes used by clients. When using WPA-PSK or WPA2-PSK, be sure to define the shared key for the Wireless-N Access Point/Repeater and all its clients. (Default: Disable)

- **WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is TKIP.
- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is AES.
- **WPA-PSK_WPA2-PSK** — Clients using WPA or WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type is TKIP/AES.
- **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)
  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

- **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

- **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

- **Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

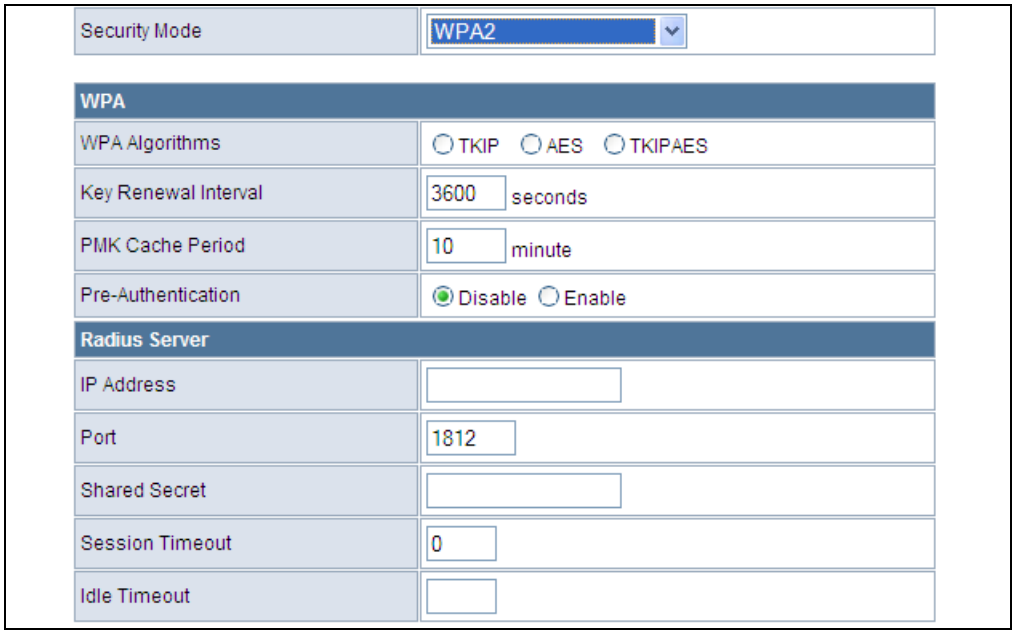
- **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

WPA ENTERPRISE MODE

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an "enterprise" and "personal" mode of operation.

For enterprise deployment, WPA and WPA2 use IEEE 802.1X for user authentication and require a RADIUS authentication server to be configured on the wired network. Data encryption keys are automatically generated and distributed to all clients connected to the network.

Figure 23: Security Mode - WPA



The following items are displayed in this section on this page:

Security Mode — Configures the WPA and WPA2 security modes used by clients. When using WPA or WPA2, be sure there is a RADIUS server in the connected wired network, and that the RADIUS settings are configured. See "IEEE 802.1X and RADIUS" on page 49 for more information. (Default: Disable)

- **WPA** — Clients using WPA with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is TKIP.
- **WPA2** — Clients using WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type for WPA is AES.
- **WPA1_WPA2** — Clients using WPA or WPA2 with an 802.1X authentication method are accepted for authentication. The default data encryption type is TKIP/AES.
- **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)
  - **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
  - **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AES-

CCMP) provides extremely robust data confidentiality using a 128-bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

  - **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

- **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

- **PMK Cache Period** — WPA2 provides fast roaming for authenticated clients by retaining keys and other security information in a cache, so that if a client roams away from an access point and then returns reauthentication is not required. This parameter sets the time for deleting the cached WPA2 Pairwise Master Key (PMK) security information. (Default: 10 minutes)

- **Pre-Authentication** — When using WPA2, pre-authentication can be enabled that allows clients to roam to another access point and be quickly associated without performing full 802.1X authentication. (Default: Disabled)

IEEE 802.1X AND RADIUS

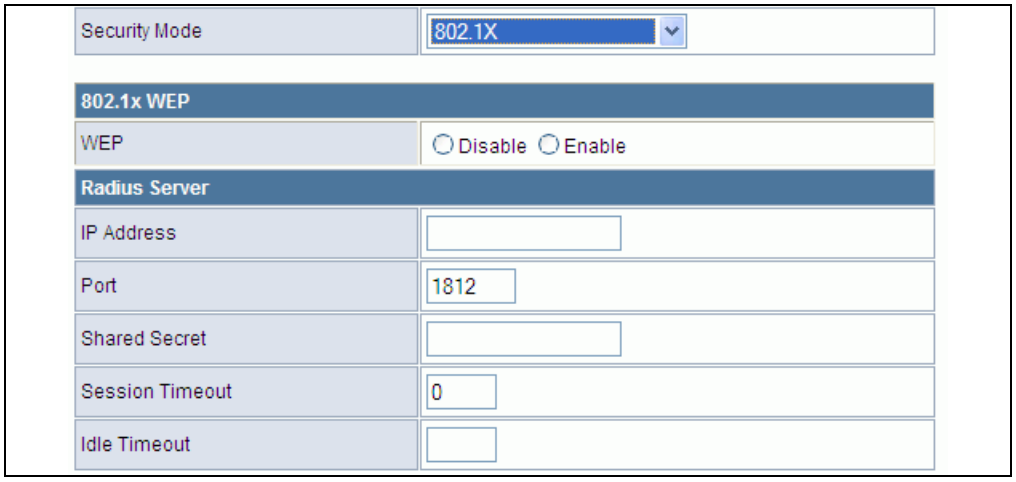
IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network.

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.

NOTE: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

Figure 24: Security Mode - 802.1X



The following items are displayed in this section on this page:

Security Mode — Configures the 802.1X security mode used by clients. When using 802.1X, either with WPA/WPA2 or on its own, be sure there is a configured RADIUS server in the connected wired network. (Default: Disable)

802.1X WEP: Selects WEP keys for data encryption. When enabled, WEP encryption keys are automatically generated by the RADIUS server and distributed to all connected clients. (Default: Disabled)

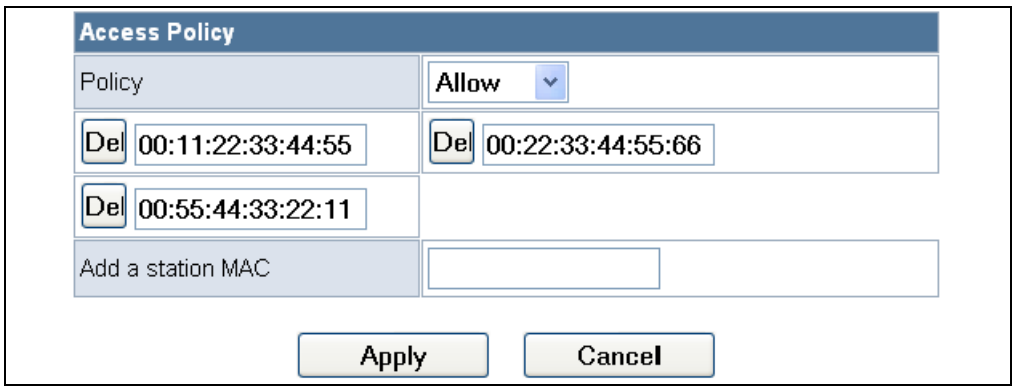
RADIUS Server — Configures RADIUS server settings.

- **IP Address** — Specifies the IP address of the RADIUS server.
- **Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Session Timeout** — Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 0)
- **Idle Timeout** — Sets the maximum time (in seconds) of client inactivity before a session is terminated.

ACCESS POLICY

The Wireless-N Access Point/Repeater provides a MAC address filtering facility. The access policy can be set to allow or reject specific station MAC addresses. This feature can be used to connect known wireless devices that may not be able to support the configured security mode.

Figure 25: Access Policy



The following items are displayed in this section on this page:

- **Access Policy** — The access policy can be set to allow or reject specific station MAC addresses.
- **Add a station MAC —** Enter the MAC address of the station that you want to filter. MAC addresses must be entered in the format xx:xx:xx:xx:xx:xx.

WIRELESS DISTRIBUTION SYSTEM (WDS)

The radio interface can be configured to operate in a mode that allows it to forward traffic directly to other Wireless Access Point/Repeater units. This feature can be used to extend the range of the wireless network to reach remote clients, or to link disconnected network segments to an Internet connection.

To set up links between units, you must configure the Wireless Distribution System (WDS) forwarding table by specifying the wireless MAC address of all units to which you want to forward traffic.

NOTE: All units in a WDS wireless network must be configured with the same SSID and use the same radio channel. Also each WDS link must be configured with the same encryption key on both units in the link.

Up to four WDS links can be specified for each unit in the WDS network. The following figures illustrate an example WDS network. Figure 26 shows the manual set up of MAC addresses for units in the WDS network. Figure 27 shows the basic configuration required on each unit in the WDS network.

Figure 26: Manual WDS MAC Address Configuration

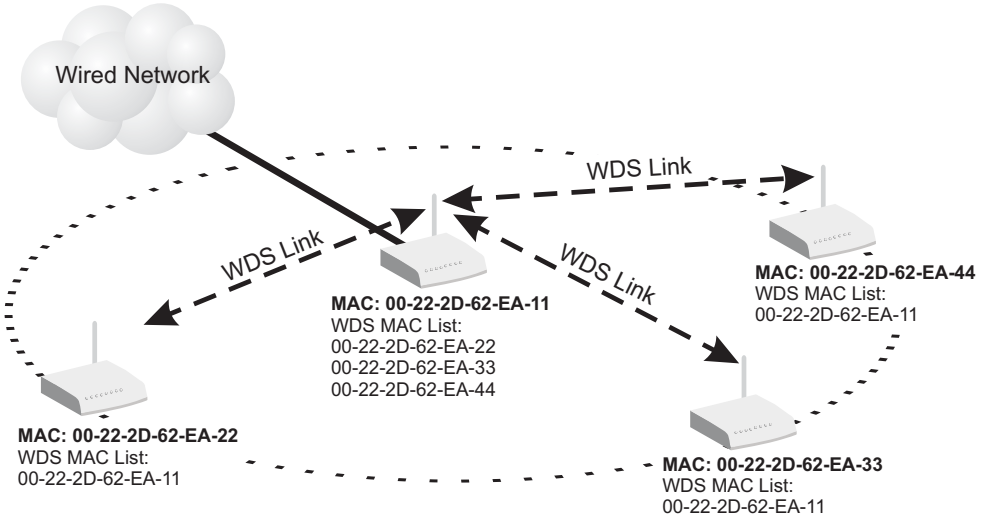
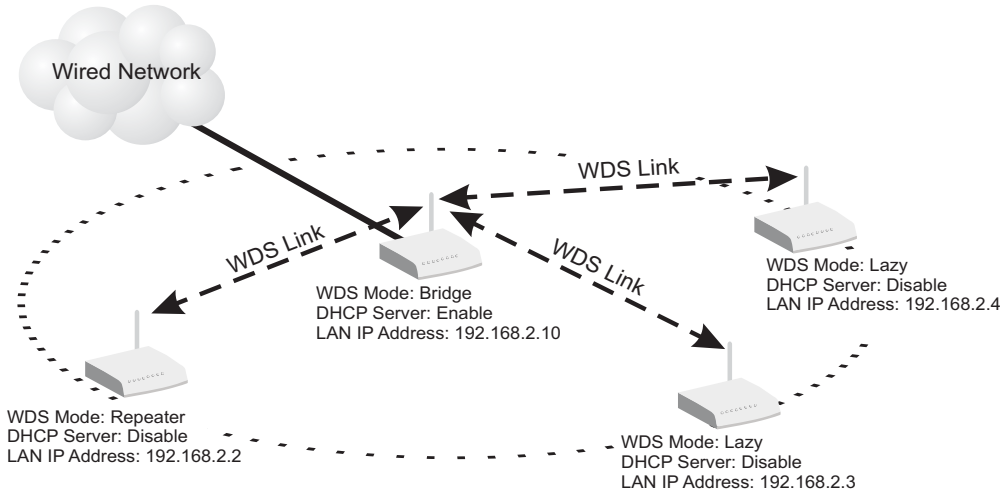
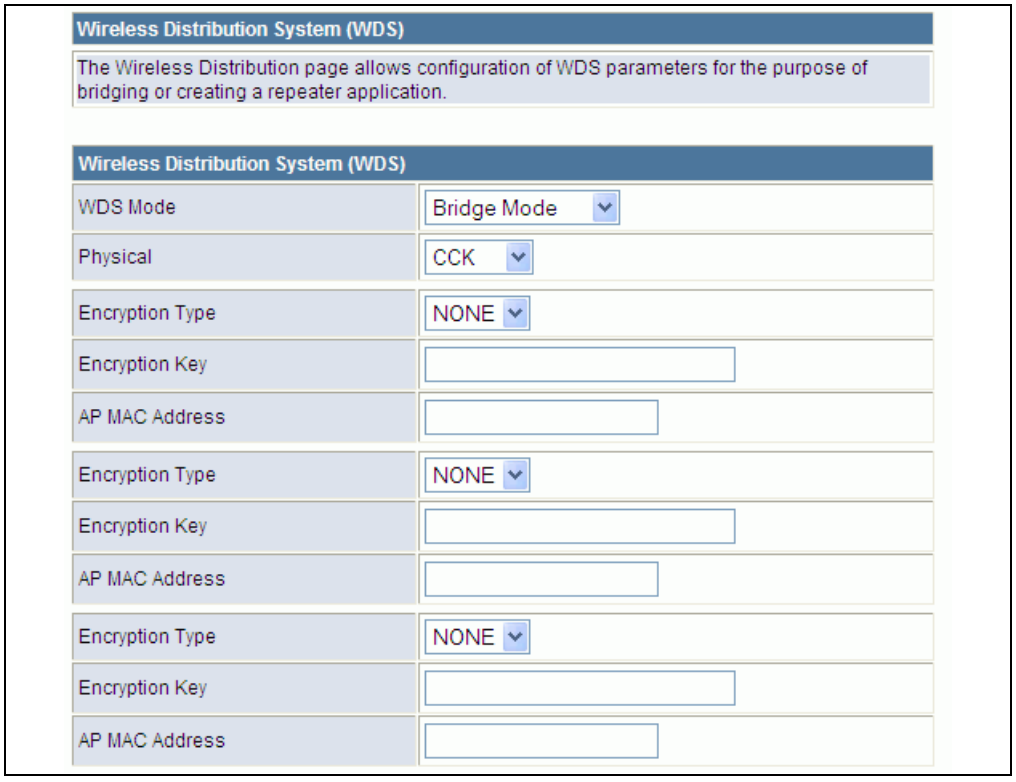


Figure 27: WDS Configuration Example



NOTE: When using WDS Lazy mode in the network, at least one unit must be set to Bridge or Repeater mode.

Figure 28: WDS Configuration



The WDS settings configure WDS related parameters. Up to four MAC addresses can be specified for each unit in the WDS network. WDS links may either be manually configured (Bridge and Repeater modes) or auto-discovered (Lazy mode).

The following items are displayed on this page:

- **WDS Mode** — Selects the WDS mode of the SSID. (Options: Disable, Lazy, Bridge, Repeater. Default: Disable)
  - **Disable**: WDS is disabled.
  - **Lazy**: Operates in an automatic mode that detects and learns WDS peer addresses from received WDS packets, without the need to configure a WDS MAC list entry. This feature allows the Wireless-N Access Point/Repeater to associate with other Wireless-N Access Point/Repeaters in the network and use their WDS MAC list. Lazy mode requires one other Wireless-N Access Point/Repeater within the wireless network that is configured in Bridge or Repeater mode, and has a configured MAC address list.
  - **Bridge**: Operates as a standard bridge that forwards traffic between WDS links (links that connect to other units in Repeater or Lazy mode). The MAC addresses of WDS peers must be configured on the Wireless-N Access Point/Repeater.

- **Repeater**: Operates as a wireless repeater, extending the range for remote wireless clients and connecting them to an AP connected to the wired network. The MAC addresses of WDS peers must be configured on the Wireless-N Access Point/Repeater.

- **Physical** — The radio media coding used on all WDS links. CCK corresponds to 11b, OFDM corresponds to 11g, and HTMIX corresponds to 11n.

- **Encryption Type** — The data encryption used on the WDS link. Be sure that both ends of a WDS link are configured with the same encryption type and key. (Options: None, WEP, TKIP, AES. Default: None)

- **Encryption Key** — The encryption key for the WDS link. The key type and length varies depending on the encryption type selected. For WEP, enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. For TKIP or AES, enter a password key phrase of between 8 to 63 ASCII characters, which can include spaces, or specify exactly 64 hexadecimal digits.

- **AP MAC Address** — The MAC address of the other Wireless-N Access Point/Repeater in the WDS link.

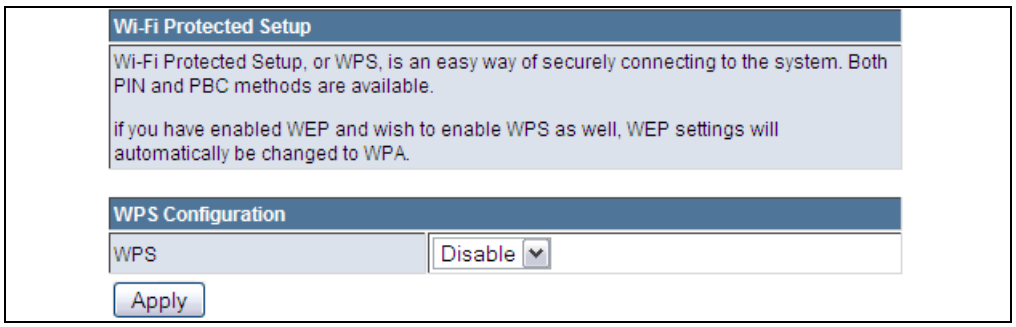
WI-FI PROTECTED SETUP (WPS)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the Wireless-N Access Point/ Repeater can be pressed at any time to allow a single device to easily join the network.

The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button.

Click on “Wireless Settings,” followed by “WPS”.

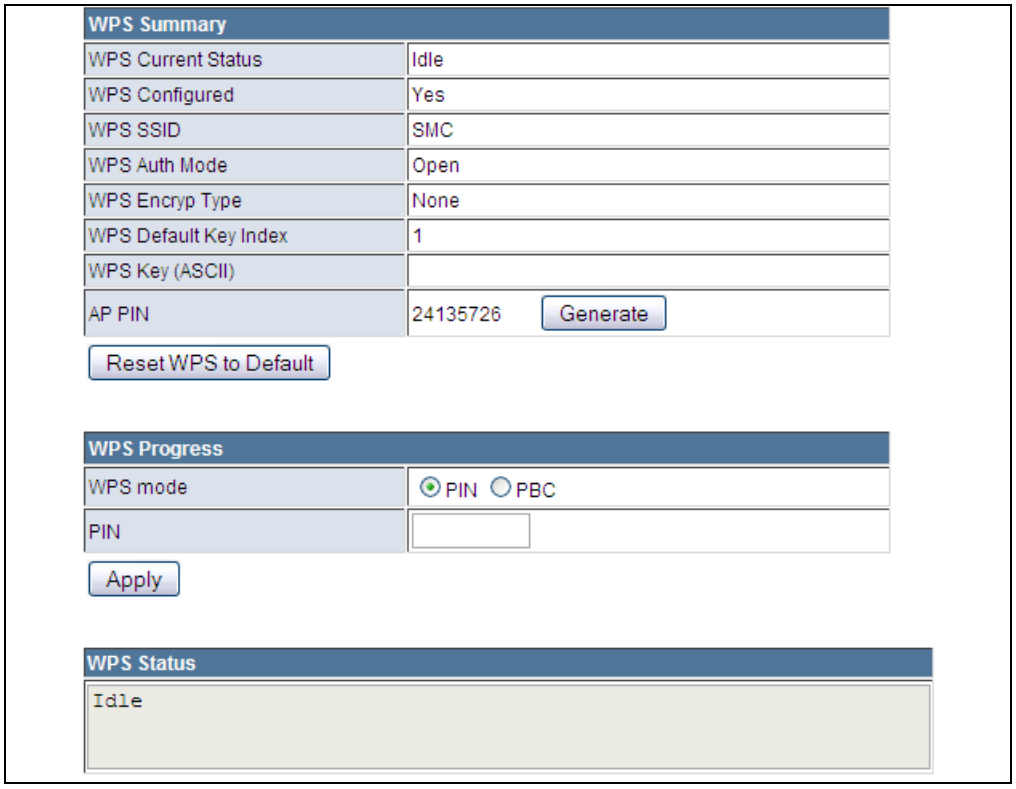
Figure 29: Enabling WPS



The following items are displayed on this page:

- **WPS** — Enables WPS, locks security settings, and refreshes WPS configuration information. (Default: Disabled)

Figure 30: WPS Configuration



The following items are displayed on this page:

WPS Summary — Provides detailed WPS statistical information.

- **WPS Current Status** — Displays if there is currently any WPS traffic connecting to the Wireless-N Access Point/Repeater. (Options: Start WSC Process; Idle)
- **WPS Configured** — States if WPS for wireless clients has been configured for this device.
- **WPS SSID** — The service set identifier for the unit.
- **WPS Auth Mode** — The method of authentication used.
- **WPS Encryp Type** — The encryption type used for the unit.
- **WPS Default Key Index** — Displays the WEP default key (1~4).
- **WPS Key (ASCII)** — Displays the WPS security key (ASCII) which can be used to ensure the security of the wireless network.

- **AP PIN** — Displays the PIN Code for the Wireless-N Access Point/ Repeater. The default is exclusive for each unit.

- **Reset WPS to Default** — Resets the WPS settings to factory default values.

WPS Config — Configures WPS settings for the Wireless-N Access Point/ Repeater.

- **WPS Mode** — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:

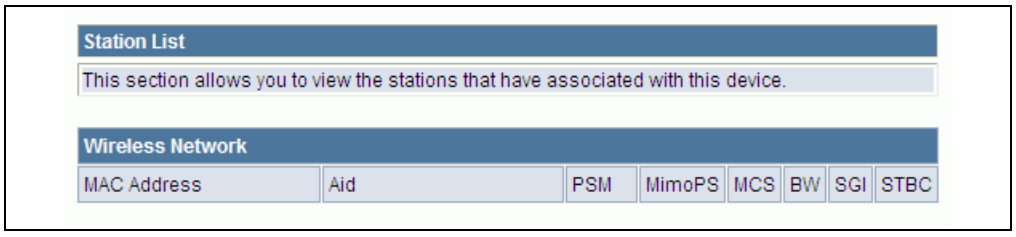
  - **PIN**: The Wireless-N Access Point/Repeater, along with other WPS devices, such as notebook PCs, cameras, or phones, all come with their own eight-digit PIN code. When one device, the WPS enrollee, sends a PIN code to the Wireless-N Access Point/Repeater, it becomes the WPS registrar. After configuring PIN-Code information you must press "Apply" to send the beacon, after which you have up to two minutes to activate WPS on devices that need to join the network.

  - **PBC**: This has the same effect as pressing the physical WPS button that is located on the front of the Wireless-N Access Point/Repeater. After checking this option and clicking "Apply" you have up to two minutes to activate WPS on devices that need to join the network.

STATION LIST

Displays the station information which associated to this Wireless-N Access Point/Repeater.

Figure 31: Station List



7 ADMINISTRATION SETTINGS

The Wireless-N Access Point/Repeater's Administration Settings allow you to configure a management access password, set the system time, upgrade the system software, display the system status and statistics.

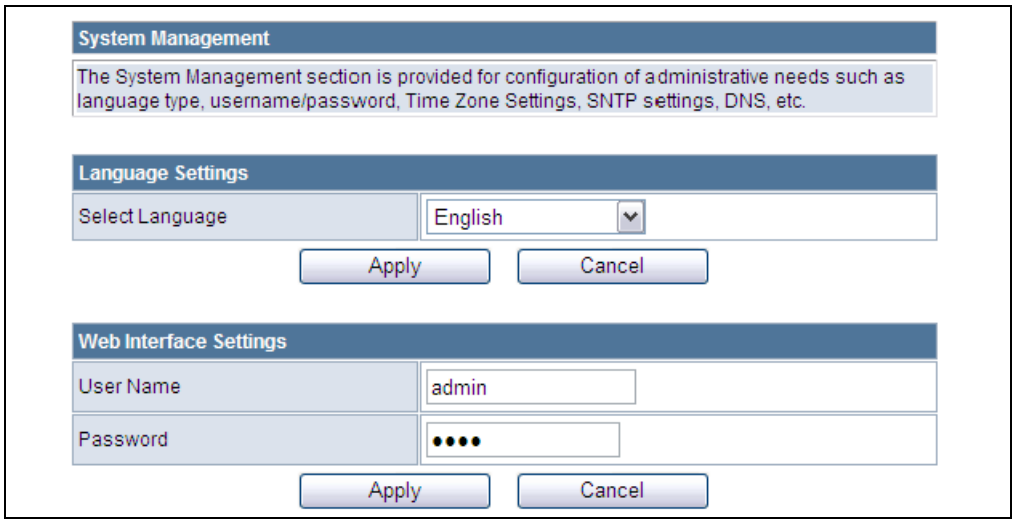
Administration Settings contains the following sections:

- "System Management" on page 57
- "Firmware Upgrade" on page 59
- "Configuration Settings" on page 60
- "System Status" on page 61
- "Statistics" on page 62
- "System Log" on page 63

SYSTEM MANAGEMENT

The System Management commands allow you to change the language settings displayed in the interface, and change the user name and password.

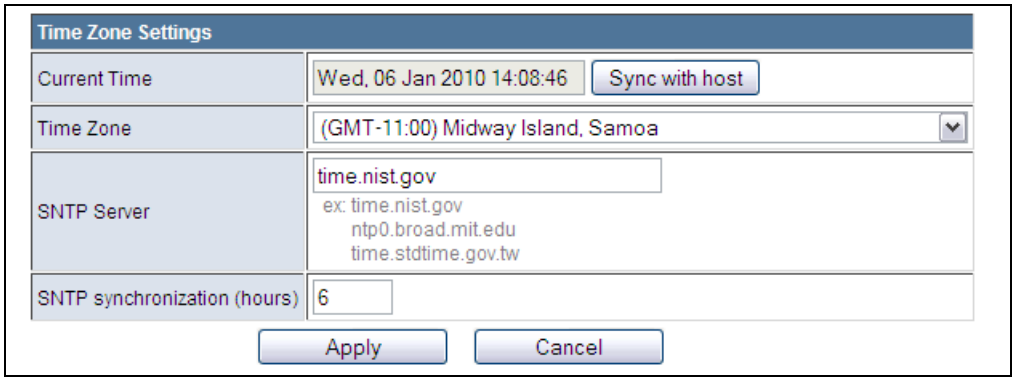
Figure 32: System Management



The following items are displayed in the first two sections on this page:

- **Language Settings** — You can change the language displayed in web interface. Select the language of your choice from the drop-down list, then click "Apply". (Options: English, Traditional Chinese, Simple Chinese, or Korean. Default: English)
- **Web Interface Settings** — To protect access to the management interface, you need to configure a new administrator's user name and password as soon as possible. If a new user name and password are not configured, then anyone having access to the Wireless-N Access Point/Repeater may be able to compromise the unit's security by entering the default values.
  - **User Name** — The name of the user. The default name for access to the unit is "admin". (Length: 3-16 characters, case sensitive)
  - **Password** — The password for management access. The default password preset for access to the unit is "smcadmin" (Length: 3-16 characters, case sensitive)
- **Time Zone Settings** — The System Management page allows you to manually configure time settings or enable the use of a Simple Network Time Protocol (SNTP) or NTP server.

Figure 33: Time Zone Settings



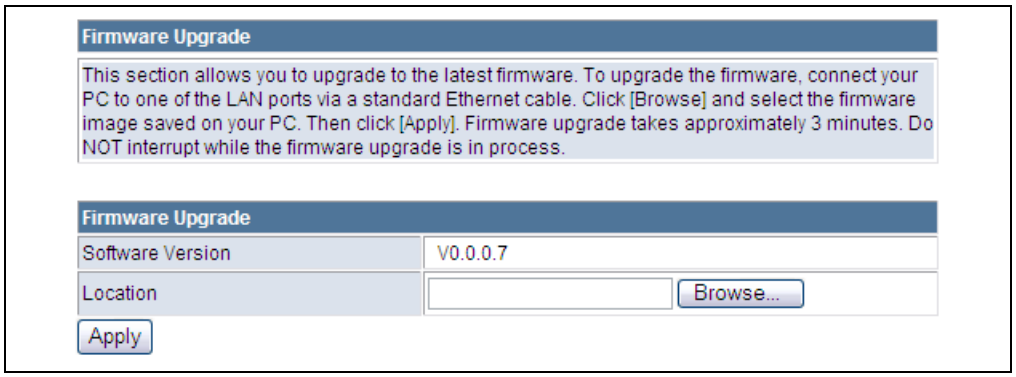
The following items are displayed in this section on this page:

- **Current Time** — Displays the current system time on the unit.
- **Sync with host —** Updates the unit's time from the web management PC's system time.
- **Time Zone** — Specifies the time zone in relation to Greenwich Mean Time (GMT).
- **SNTP Server** — The IP address or URL of the NTP server to be used.
- **SNTP synchronization —** Sets the SNTP sycnronization in hours.

FIRMWARE UPGRADE

You can update the Wireless-N Access Point/Repeater firmware by using the Firmware Update facility.

Figure 34: Firmware Upgrade



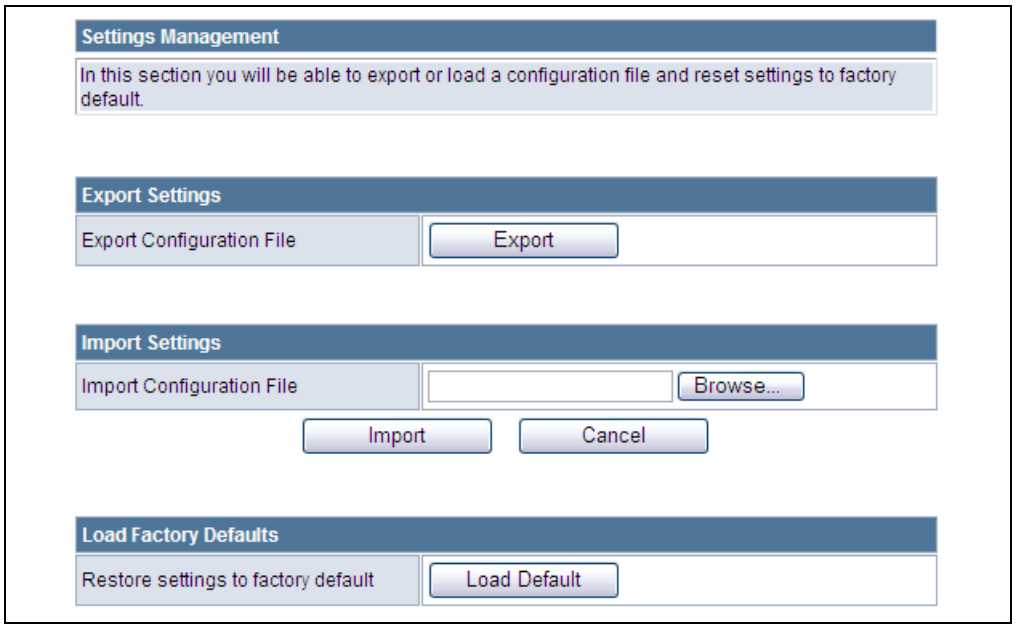
The following items are displayed on this page:

- **Firmware Upgrade** — Allows you to upload new firmware manually by specifying a file path. Make sure the firmware you want to use is on the local computer by clicking Browse to search for the firmware to be used for the update.
  - **Software Version** — The current version number of the firmware.
  - **Browse** — Opens a directory on the local hard drive for specifying the path of the file to upload.
  - **Apply** — Starts the upload procedure.

CONFIGURATION SETTINGS

The Configuration Setting page allows you to save the Wireless-N Access Point/Repeater's current configuration or restore a previously saved configuration back to the device.

Figure 35: Configuration Settings



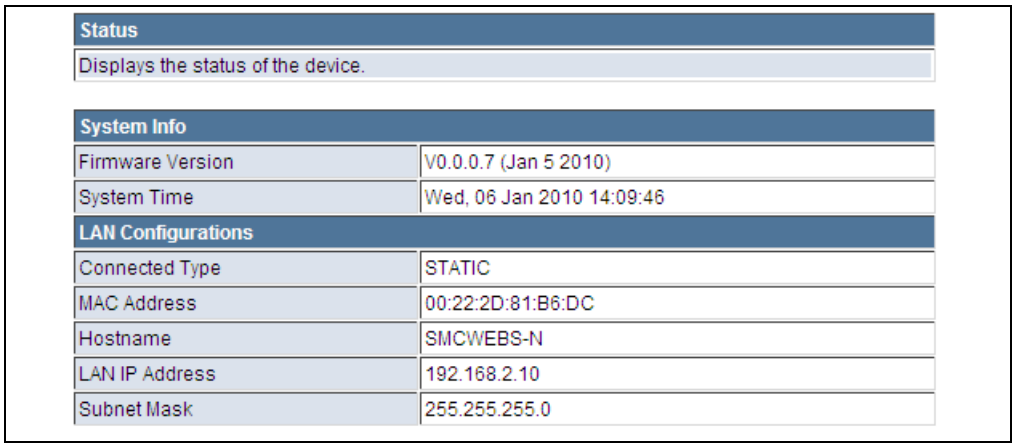
The following items are displayed on this page:

- **Export Settings** — Saves the current configuration to a file locally.
- **Import Settings** — Allows the user to load previously saved configuration files from a local source.
- **Load Factory Defaults** — Restores the factory defaults.

SYSTEM STATUS

The System Information page displays basic system information and the displayed settings are for status information only and are not configurable on this page. This information is split into the three sections that follow.

Figure 36: System Status



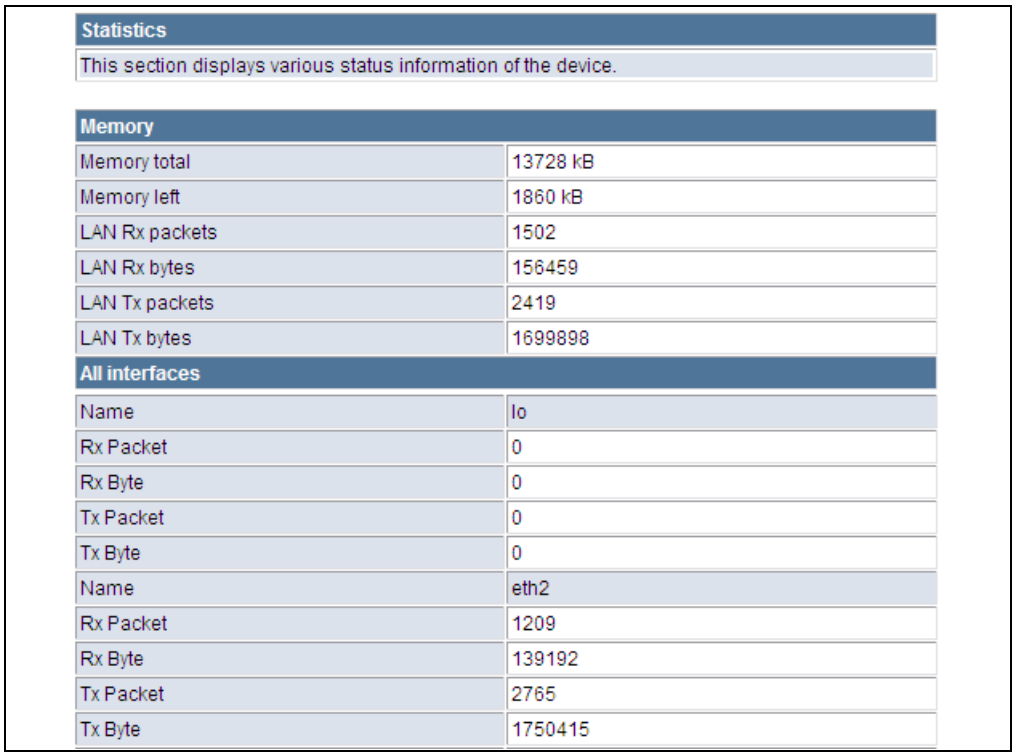
The following items are displayed on this page:

- **System Info** — Displays the basic system information.
  - **Firmware Version** — The version number of the current Wireless-N Access Point/Repeater software.
  - **System Time** — Length of time the management agent has been up, specified in hours and minutes.
- **LAN Configurations** — Displays the basic WAN information:
  - **Connected Type** — Displays the WAN connected mode.
  - **MAC Address** — The shared physical layer address for the Wireless-N Access Point/Repeater's LAN ports.
  - **Hostname** — The hostname of the STATIC or DHCP client.
  - **LAN IP Address** — Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.2.10.
  - **Subnet Mask** — The mask that identifies the host address bits used for routing to the WAN port.

STATISTICS

The Wireless-N Access Point/Repeater Traffic Statistics - Interfaces window displays received and transmitted packet statistics for all interfaces on the Wireless-N Access Point/Repeater.

Figure 37: Statistics



Statistics

This section displays various status information of the device.

Memory	
Memory total	13728 kB
Memory left	1860 kB
LAN Rx packets	1502
LAN Rx bytes	156459
LAN Tx packets	2419
LAN Tx bytes	1699898
All interfaces	
Name	lo
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	eth2
Rx Packet	1209
Rx Byte	139192
Tx Packet	2765
Tx Byte	1750415

The following items are displayed on this page:

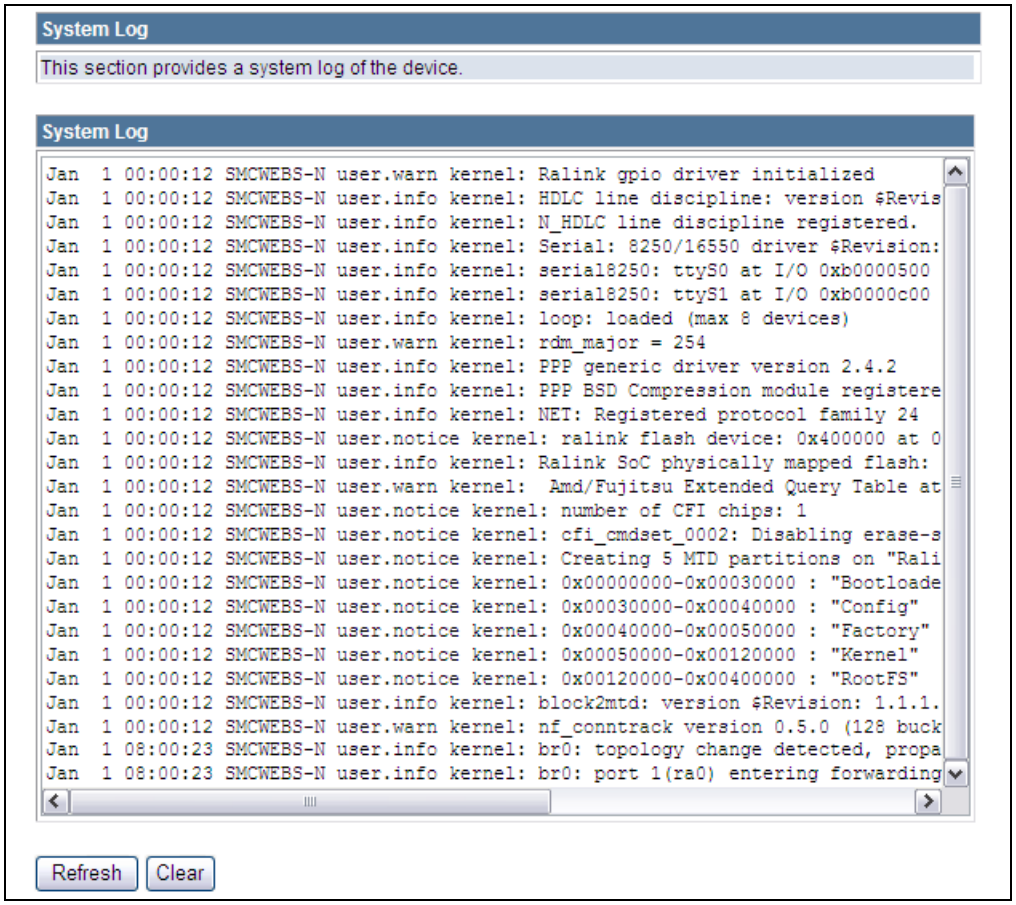
- **Memory total** — The total memory of this Wireless-N Access Point/ Repeater.
- **Memory left** — The available memory of this Wireless-N Access Point/ Repeater.
- **All Interfaces** — Displays the interface on which traffic is being monitored.
- **Rx packets** — Displays the total number of packets received by the specified interface.
- **Rx bytes** — Displays the total number of bytes transmitted by the specified interface.
- **Tx packets** — Displays the total number of packets transmitted by the specified interfaces.

- **Tx bytes** — Displays the total number of bytes transmitted by the specified interface.

SYSTEM LOG

The Wireless-N Access Point/Repeater supports a logging process that controls error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating Wireless-N Access Point/Repeater and network problems. The System Log page displays the latest messages logged in chronological order, from the newest to the oldest. Log messages saved in the Wireless-N Access Point/Repeater's memory are erased when the device is rebooted.

Figure 38: System Log



The following items are displayed on this page:

- **System Log** — Displays the latest log messages in chronological order, from the newest to the oldest.
- **Refresh** — Sends a request to add the latest entries to the System Log Table.

- **Clear** — Removes the current system log messages from the System Log Table.

Section III

Appendices

This section provides additional information and includes these items:

- "Troubleshooting" on page 66
- "Hardware Specifications" on page 68
- "Cables and Pinouts" on page 70
- "Glossary" on page 77
- "Index" on page 81

A TROUBLESHOOTING

DIAGNOSING LED INDICATORS

Table 4: LED Indicators

Symptom	Action
Power/LAN LEDs are off	◆ The AC power adapter may be disconnected. Check connections between the Access Point/Repeater, the power adapter, and the wall outlet.
WLAN LED is off	◆ The access point radio has been disabled through it's web management interface. Access the management interface using a web browser to enable the radio.
LAN LEDs are off (when port connected)	◆ Verify that the Access Point/Repeater is powered on. ◆ Be sure cables are plugged into both the Access Point/Repeater and corresponding PC. ◆ Verify that the proper cable type is used and its length does not exceed specified limits. ◆ Check the cable connections for possible defects. Replace the defective cable if necessary.

BEFORE CONTACTING TECHNICAL SUPPORT

Check the following items before you contact local Technical Support.

1. If the Access Point/Repeater cannot be configured using a web browser:

   - Be sure to have configured the Access Point/Repeater with a valid IP address, subnet mask and default gateway.
   - Check that you have a valid network connection to the Access Point/Repeater and that the Ethernet port or the wireless interface that you are using has not been disabled.
   - If you are connecting to the Access Point/Repeater through the wired Ethernet interface, check the network cabling between the management station and the Access Point/Repeater. If you are connecting to Access Point/Repeater from a wireless client, ensure that you have a valid connection to the Access Point/Repeater.

2. If you forgot or lost the password:

   - Set the Access Point/Repeater to its default configuration by pressing the reset button on the back panel for 5 seconds or more.

Then use the default user name "admin" and password "smcadmin" to access the management interface.

3. If all other recovery measure fail, and the Access Point/Repeater is still not functioning properly, take any of these steps:

   - Reset the Access Point/Repeater's hardware using the web interface, or through a power reset.

B HARDWARE SPECIFICATIONS

PORT INTERFACES	LAN 1~4: 1 10/100BASE-TX port, RJ-45 connector, auto MDI/X (100-ohm, UTP cable; Category 5 or better)
AC POWER ADAPTER	Input: 100~240 VAC, 50/60 Hz Output: 5 V/ 1 A
LED INDICATORS	Power, WLAN (Wireless Local Area Network), WPS (Wi-Fi Protected Setup), LAN 1~4 (Local Area Network).
NETWORK MANAGEMENT	Web-browser
TEMPERATURE	Operating: 0 to 40 °C (32 to 104 °F) Storage: -20 to 70 °C (32 to 158 °F)
HUMIDITY	20% to 85% (non-condensing)
PHYSICAL SIZE	136 X 90.8 X 28.5 mm
WEIGHT	157 g (5.54 oz)
RADIO	FCC Part 15C (Section 15.247) EN 301 489-1 V1.8.1 (2008-04) EN 301 489-17 V1.3.2 (2008-04) LP0002
EMC	FCC Part 15B EN 55022:2006 + A1:2007 EN 55024:1998 + A1:2001 + A2:2003
SAR	FCC IEEE C95.1 EN 50385 (2002)

SAFETY EN 60950-1 (2006)

ENVIRONMENTAL ETSI EN 300 019-2-1 Class 1.2 (Storage)
ETSI EN 300 019-2-2 Class 2.3 (Packaged)
ETSI EN 300 019-2-3 Class 3.2 (Operating)

C CABLES AND PINOUTS

TWISTED-PAIR CABLE ASSIGNMENTS

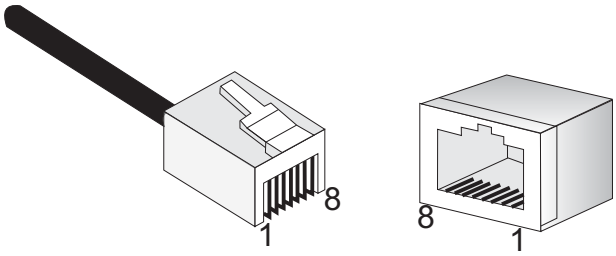
For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. For 1000BASE-T connections the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

NOTE: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

CAUTION: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

Figure 39: RJ-45 Connector



10/100BASE-TX PIN ASSIGNMENTS

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through or crossover cables for all network connections to PCs, switches, or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable.

Table 5: 10/100BASE-TX MDI and MDI-X Port Pinouts

PIN	MDI Signal Name[a]	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4, 5, 7, 8	Not used	Not used

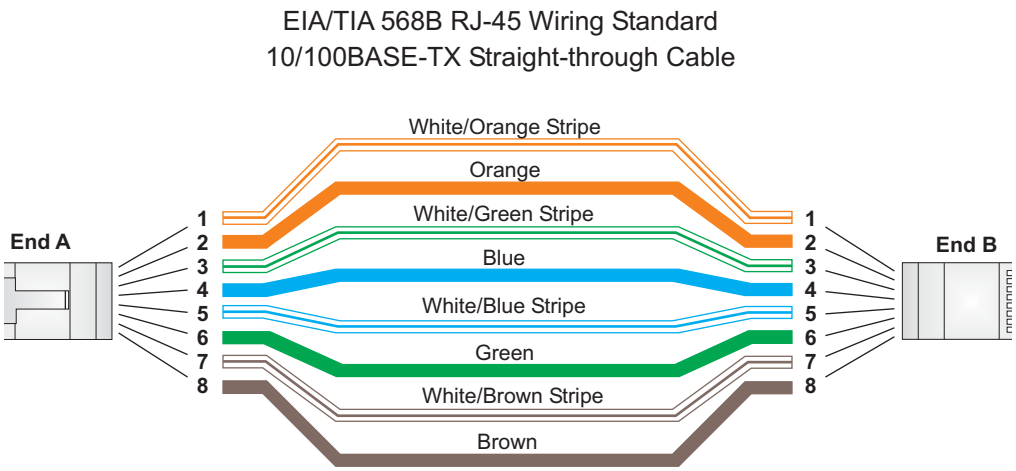
a. The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

STRAIGHT-THROUGH WIRING

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through. (When auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

Figure 40: Straight-through Wiring

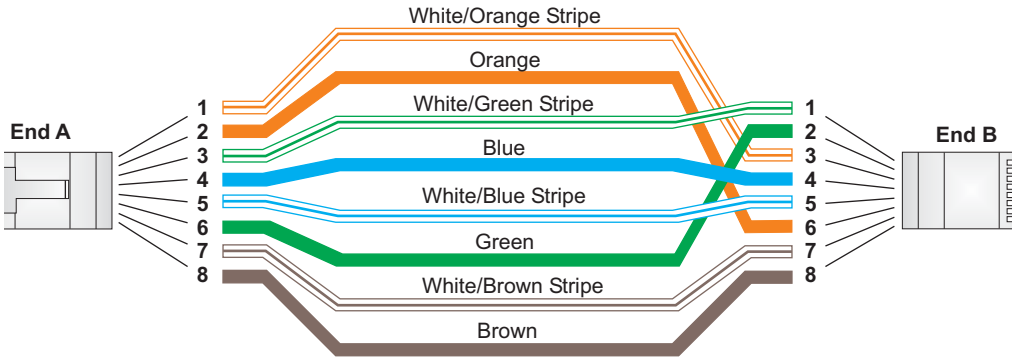


CROSSOVER WIRING

If the twisted-pair cable is to join two ports and either both ports are labeled with an "X" (MDI-X) or neither port is labeled with an "X" (MDI), a crossover must be implemented in the wiring. (When auto-negotiation is enabled for any RJ-45 port on this switch, you can use either straight-through or crossover cable to connect to any device type.)

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet connections.

Figure 41: Crossover Wiring



D LICENSE INFORMATION

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GLOSSARY

10BASE-T IEEE 802.3-2005 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX IEEE 802.3-2005 specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

1000BASE-T IEEE 802.3ab specification for 1000 Mbps Gigabit Ethernet over four pairs of Category 5 or better UTP cable.

ACCESS POINT An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

AES Advanced Encryption Standard: An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

AUTHENTICATION The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

BACKBONE The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

BEACON A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

BROADCAST KEY Broadcast keys are sent to stations using dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on

the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

ENCRYPTION Data passing between the access point and clients can use encryption to protect from interception and evesdropping.

ETHERNET A popular local area data communications network, which accepts transmission from computers and terminals.

FTP File Transfer Protocol: A TCP/IP protocol used for file transfer.

HTTP Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11B A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11G A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

INFRASTRUCTURE An integrated wireless and wired LAN is called an infrastructure configuration.

LAN Local Area Network: A group of interconnected computers and support devices.

MAC ADDRESS The physical layer address used to uniquely identify network nodes.

NTP Network Time Protocol: NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OPEN SYSTEM A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

ODFM Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

SSID Service Set Identifier: An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

SESSION KEY Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

SHARED KEY A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

SNTP Simple Network Time Protocol: SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

TKIP Temporal Key Integrity Protocol: A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

TFTP Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

VAP Virtual Access Point: Virtual AP technology multiplies the number of Access Points present within the RF footprint of a single physical access device. With Virtual AP technology, WLAN users within the device.s footprint can associate with what appears to be different access points and their associated network services. All the services are delivered using a single radio channel, enabling Virtual AP technology to optimize the use of limited WLAN radio spectrum.

WI-FI PROTECTED ACCESS WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

WEP Wired Equivalent Privacy: WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA-PSK WPA Pre-shared Key: WPA-PSK can be used for small office networks with a limited number of users that may not need a high level of security. WPA-PSK provides a simple security implementation that uses just a pre-shared password for network access.

INDEX

NUMERICS

10/100BASE-TX pin assignments 71
802.11n settings 34

A

access categories, WMM 41
access point connections 21
access policy settings 51
AES encryption 47
aggregate MSDU 37
AP isolation 36
authentication options 44

B

beacon interval 39
BG protection mode 39
buttons
    WPS 20

C

channel setting 36
common web page buttons 28
configuration settings 60
crossover cables 72

D

data beacon rate 39
default IP address 26
default Key, WEP 45
Description of Capabilities 17
desktop mounting 25
dimensions, physical 68
DTIM setting 39

E

encryption options 44
enterprise mode, WPA 47
Ethernet port 20
export configuration 60
extension channel setting 37

F

factory default 20
factory defaults, resetting 60
firmware upgrade 59
fragmentation threshold 39
frequency setting 36

G

guard interval 37

H

Hardware Description 18
horizontal surface mounting 25
HT channel bandwidth 37

I

import configuration 60
information, system 61
Introduction 17
IP address, default 26

K

Key Hardware Features 17

L

LAN ports 20
LAN settings 32
language settings 28, 58
Lazy Mode, WDS 53
LED indicators 19
    troubleshooting 66
license information 73
LLTD 33
local network settings 32
location selection 24
logging, system 63
login defaults 26
login page 26

M

MAC address filtering 51
management interface, login defaults 26
MCS setting 37
MDI/MDI-X operation 20
messages, logging 63
mounting 25

mounting on a wall 24
multicast-to-unicast convertion 43
multiple SSID 36

N

network name, wireless 34, 36
network statistics 62

O

open system 43

P

Package Contents 18
password
  default 26
  setting 58
PBC mode, WPS 56
physical size 68
PIN code, WPS 56
pinouts, cable 70
PMK cache period 49
power connector 20
preamble, short 40
pre-authentication 49
protection mode 39

Q

Quality of Service 40

R

radio mode 35
radio settings 34
radio standards 68
RADIUS 49
repeater operation 22
Reset Button 20
restoring defaults 60
reverse direction grant 37
RJ-45 connector pins 70
RTS threshold 39

S

screws for mounting 24
security features 17
security, wireless 43
setup wizard 28
shared secret, RADIUS 50
slot time 40
slots 24
SNTP 58
software upgrade 59
specifications, hardware 68
SSID 34, 36
standards, radio 68
station list, wireless 56
Statistics 62
statistics, system 62
status of system 61
straight-through cables 71
system defaults 60
system log 63
system requirements 23
System Status 61
system time 58

T

table mounting 25
temperature, operating 68
time settings 58
time zone setting 58
TKIP encryption 46
traffic statistics 62
troubleshooting 66, 73
twisted-pair cable assignments 70

U

upgrading software 59
UPNP 33
username setting 58
username, default 26
UTP cable pinouts 71

V

VAP interfaces 34

W

wall mounting 24
WDS operation 22
WDS settings 51
web browser 23
web IP address 26
web login 26
WEP security 44
Wi-Fi Multimedia 40
Wi-Fi network operation 21
wireless client list 56
wireless network mode 35
wireless settings, basic 34
WLAN security 43
WMM 40
WPA pre-shared key 46
WPS button 20
WPS security 54

SMC® Networks

TECHNICAL SUPPORT
From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: (800) SMC-4-YOU / (949) 679-8000
Fax: (949) 679-1481

English: Technical Support information available at www.smc.com

English (For Asia Pacific): Technical Support information available at www.smc-asia.com

Deutsch: Technischer Support und weitere Information unter www.smc.com

Español: En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

Français: Informations Support Technique sur www.smc.com

Português: Informações sobre Suporte Técnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgängligt på www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym sa dostepne na www.smc.com

Čeština: Technicka podpora je dostupna na www.smc.com

Magyar: Műszaki tamogat informacio elerhető -on www.smc.com

简体中文：技术支持讯息可通过www.smc-prc.com查询

繁體中文：產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smc-asia.com을 참고하시기 바랍니다

INTERNET
E-mail address: www.smc.com→ Support→ By email
Driver updates: www.smc.com→ Support→ Downloads

World Wide Web: http://www.smc.com/

SMCWEBS-N

20 Mason • Irvine, CA 92618 • Phn: (949) 679-8000 • www.smc.com